

ActiveXperts Network Monitor 7.2

Administrator's Manual

January 2010

© 2003-2010 - ActiveXperts® Software

<http://www.activexperts.com>

contact@activexperts.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of ActiveXperts Software B.V. Products named herein may be trademarks of their respective manufacturers and are hereby recognized. Trademarked names are used editorially, to the benefit of the trademark owner, with no intent to infringe on the trademark.

Version 7.2 last updated: September, 2009

1. INTRODUCING ACTIVEXPERTS NETWORK MONITOR	1
1.1. PRODUCT OVERVIEW	1
1.2. PRODUCT FEATURES	1
1.3. BUILT-IN MONITORING CHECKS	3
1.4. CUSTOM MONITORING CHECKS	5
1.5. NOTIFICATIONS	6
1.6. ACTIONS	7
1.7. ERRORS, FAILURES AND RECOVERY	7
1.8. MAINTENANCE SCHEDULES	9
2. INSTALLING ACTIVEXPERTS NETWORK MONITOR	10
2.1. SOFTWARE COMPONENTS	10
2.2. INSTALLING ACTIVEXPERTS NETWORK MONITOR	11
2.3. INSTALLING MANAGEMENT CONSOLE ON A WORKSTATION	14
3. CONFIGURING ACTIVEXPERTS NETWORK MONITOR	16
3.1. INTRODUCTION	16
3.2. ACTIVEXPERTS NETWORK MONITOR MANAGER	16
3.3. ACTIVEXPERTS NETWORK MONITOR QUICK CONFIGURATION WIZARD	18
3.4. IMPORT, EXPORT AND CLEAR CONFIGURATION SETTINGS	18
3.5. RENAMING COMPUTERS	19
3.6. CONFIGURING MONITORING CHECKS	19
3.7. OPTIONS	20
3.8. NOTIFICATIONS	21
3.9. E-MAIL NOTIFICATIONS	23
3.10. NETWORK NOTIFICATIONS	24
3.11. SMS NOTIFICATIONS	25
3.12. PAGER NOTIFICATIONS	26
3.13. SNMP TRAP NOTIFICATIONS	27
3.14. MESSAGE TEMPLATES	28
3.15. MAINTENANCE	29
3.16. DEPENDENCIES	29
3.17. BACKUP AND RESTORE	29
4. MANAGING MONITORING CHECKS	31
4.1. ADDING A NEW CHECK	31
4.2. COPY/PASTE A CHECK	31
4.3. DELETING A CHECK	31
4.4. EDITING A CHECK	31
4.5. MONITORING SERVERS IN THE SAME DOMAIN	34
4.6. MONITORING SERVERS IN THE OTHER DOMAINS	34
4.7. CONFIGURING A CHECK	34
4.8. WRITING YOUR OWN MONITORING CHECKS USING VBSCRIPT	56
4.9. WRITING YOUR OWN MONITORING CHECKS USING A LINUX/UNIX SHELL SCRIPT	60
5. MANAGING FOLDERS	62
5.1. ADDING A NEW FOLDER	62
5.2. EDITING A FOLDER	62
5.3. DELETING A FOLDER	62
6. WEB INTERFACE	63
6.1. INTRODUCTION	63
6.2. USING THE WEB INTERFACE	63
6.3. CUSTOMIZING THE WEB INTERFACE	64
7. REPORT MODULE	66

7.1. INTRODUCTION	66	
7.2. REPORT DEFINITION FILES (*.REP)	66	
7.3. CREATING A NEW REPORT MANUALLY	67	
7.4. CREATING A NEW REPORT AUTOMATICALLY (SCHEDULED)		67
7.5. CUSTOMIZING REPORTS	69	
7.6. FORMATTING REPORTS	72	
8. PERMISSIONS	74	
8.1. NO ACCESS	74	
8.2. READ-ONLY ACCESS	74	
8.3. READ/WRITE ACCESS	75	
9. TUNING THE SYSTEM	76	
9.1. INTRODUCTION	76	
9.2. CONFIGURING THE NUMBER OF THREADS	76	
9.3. LOG FILES	77	
10. TROUBLESHOOTING	78	
11. PURCHASE AND PRODUCT ACTIVATION	79	
11.1. LICENSE SCHEME	79	
11.2. PURCHASE	79	
11.3. PRODUCT ACTIVATION	80	
APPENDIX A: REPORT DATA FORMAT	1	
A.1. XML AVAILABILITY REPORTS	1	
A.2. XML DETAIL REPORTS	2	
A.3. CONTANTS	4	
APPENDIX B: WEB INTERFACE XML TAGS	6	
APPENDIX C: NOTIFICATION VARIABLES	7	

1. Introducing ActiveXperts Network Monitor

1.1. Product Overview

ActiveXperts Network Monitor is a network and server monitoring tool to allow administrators to monitor the network for failures and irregularities automatically. It can monitor all aspects of your LAN- and WAN servers, workstations and IP devices.

For years, System Administrators, Network Operators and Helpdesk Employees have relied upon the power, flexibility and reliability of the ActiveXperts Network Monitor tool.

The mission of the product is to maximize the reliability of your production servers and applications through the automatic detection and correction of problems and issues. The product runs as a service on a Windows 2008/Vista/2003/2000/XP platform, 32-bit or 64-bit.

When problems are detected, you're immediately notified by e-mail, SMS, pager, SNMP trap or network message. When a failure is detected, the network monitor tool will try to correct the problem. ActiveXperts Network Monitor consists of a Network Monitor Engine (a Windows service) and a Network Monitor Manager application.

The **Network Monitor Engine** is the service that continuously monitors the servers, workstations and IP devices in your LAN/WAN for availability. The service is also responsible for notifying, triggering actions, recovery and logging. There's no agent software required on the servers being monitored; the monitoring service uses protocols and application layers of the Operating System to do its job.

The **Network Monitor Manager application** is used to view the results and to make changes to the configuration. This Manager application allows you to visually monitor the network from any desktop PC.

The Manager application can be installed on any Windows 2000 or higher computer (workstation or server), and has different authority levels. You can for instance restrict your help desk staff to only see monitoring results, and allowing network operators to make changes to the configuration.

1.2. Product Features

▼ Monitoring features

- ◆ Monitoring various operating systems, including Windows, Linux, Unix and Novell;
- ◆ Monitoring various application services;
- ◆ Monitoring various databases, including Oracle, MS SQL, MS Access, OLE DB (ADO) compliant and ODBC compliant databases;
- ◆ Monitoring environmental data, including temperature, humidity and wetness;
- ◆ Monitoring networks, network protocols and network services;
- ◆ Ability to write custom monitoring checks VBScript (Windows) or SSH (Linux);
- ◆ Checks are processed simultaneously by the multi-threaded monitoring engine. By default, there are 30 threads to process monitoring checks simultaneously;
- ◆ The engine is self-tuning; the number of threads adapt to the number of checks to be processed per minute;

- ◆ Software is provided with powerful, pre-defined monitoring checks.

▼ Notification features

- ◆ Send out notifications upon failure and/or upon recovery;
- ◆ Native support for SMTP e-mail notifications; Outlook or IIS/CDONT are not required; Multiple character sets are supported, including English, Arabic, Chinese and Japanese; Support for a fallback SMTP server in case the primary SMTP server is not working;
- ◆ Pager Notifications; numeric Pager support through a modem connected to the local COM port; alpha-numeric Pager support by the use of SNPP providers;
- ◆ SMS Notifications; requires either a GSM modem, a subscription with an HTTP compliant SMS provider, or a subscription with an SMPP compliant SMS provider (the latter requires ActiveXperts SMS Messaging Server running on a server in the network);
- ◆ SNMP Trap Notifications; send trap notifications to an SNMP Management console; supports SNMP v1 traps and SNMP v2 or higher SNMP traps;
- ◆ NetBIOS Network Notifications (also known as "network popup" messages);
- ◆ Global and Custom Address Lists; for all notification types (E-mail, SMS, Network and Pager) a custom list can be defined, or the global Address Book can be selected;
- ◆ Templates for all notification types, including network monitor system parameter inside these templates. Notification messages can be completely customized using these templates.

▼ Action features

- ◆ Restart a service (or multiple services) upon failure;
- ◆ Reboot a server upon failure;
- ◆ Launch an executable or batch command job; use Network Monitor system parameters as arguments for the executable or batch-job;
- ◆ Launch a VBScript; Use Network Monitor system parameters as arguments for the script.

▼ Configuration

- ◆ Configuration information is stored in an MS Access database;
- ◆ Support for Import and Export of the configuration; Import and Export are guided by a Wizard;
- ◆ Default values for new monitoring checks are configurable, and can be applied to existing monitoring checks;
- ◆ Read-only mode for users that are not allowed to make changes to the configuration (for instance: help desk employees);

▼ Maintenance schedules

- ◆ Avoid servers to be considered as Failed during maintenance hours. Notifications and actions will not occur during these schedules;
- ◆ Maintenance periods can be configured globally or per check;
- ◆ Maintenance periods can be scheduled as recurrent or only once;
- ◆ Multiple maintenance schedules can be defined.

▼ Dependencies

- ◆ Avoid a flood of messages when - for instance - a router fails, by configuring dependencies;
- ◆ Servers can depend on multiple servers; dependencies are transitive.

▼ Reports

- ◆ Standard incident reports and availability reports are included;
- ◆ The 'Report Configurator' guides the user to quickly setup new report definitions. Report Definition files can be used to either create a new report from the command line (scheduled, without user intervention) or from the graphical Report Generator;
- ◆ Reports can be scheduled using the Task Scheduler;
- ◆ Reports can be e-mailed automatically, periodically;
- ◆ Support for XML, HTML and CSV ('comma separated') formatted reports;
- ◆ Particular checks, folders and results can be included/excluded from a report;

▼ Logging

- ◆ Network Monitor related information is written to the Application Log of the Event Viewer;
- ◆ Monitoring information is written to ASCII log files or any OLE DB compliant database, including MS Access and MS SQL;
- ◆ Maximum ASCII Log file size is configurable; a new log file is created when a maximum size is reached;
- ◆ Report Data is written to an MS Access database by default. A migration wizard assists the user to migrate report data to MS SQL.

▼ User Interface

- ◆ Use the Manager application to make changes to the configuration and view the monitoring results;
- ◆ The Manager application can be installed on any workstation in the network, allowing operators to monitor and configure Network Monitor from their desktop;
- ◆ The Manager application has an Explorer-like user interface, with a Folder pane, a Monitoring Checks pane and a Log pane;
- ◆ Assign Read-only permission to the people who do not need full access to the configuration. In Read-only mode, users can only view the results, but are not able to change the configuration.
- ◆ The Web Interface allows users to view the status of the network by using the Internet Browser. The Web Interface consists of a set of web pages, also called Web Views. Web Views are based on XML/XSL technology. The views are created dynamically by the Network Monitor service, and can be customized easily by modifying the corresponding XSL templates.

1.3. Built-in Monitoring Checks

ActiveXperts Network Monitor ships with powerful set of monitoring checks.

IP-related checks:

- ◆ *DNS Server* check – checks various types of DNS server records by retrieving record values and comparing them against specified values;
- ◆ *FTP* check – checks the availability of an FTP server. It can logon/logoff, change directory and check for file existence on the FTP server. It can look for patterns in an FTP file;
- ◆ *TFTP* check – checks for file existence on the TFTP server. It can look for patterns in a TFTP file;
- ◆ *HTTP/HTTPS* check – checks the availability of a website by connecting to it and matching patterns on the site; includes support for proxy servers;
- ◆ *ICMP/Ping* check – checks the availability of an IP device or computer;
- ◆ *IMAP Mail Server* check – checks the availability of an IMAP compliant e-mail server;
- ◆ *LDAP* check – performs an LDAP query and analyzes the result;

- ♦ *NNTP News Server* check – checks the availability of an NNTP News server, using the NNTP internet protocol;
- ♦ *NTP Time Server* check – checks the availability of a Time Server by sending an NTP query and analyzing the response;
- ♦ *POP3 Mail Server* check – checks the availability of a POP3 e-mail server;
- ♦ *RADIUS Server* check – checks the availability of a RADIUS authentication server;
- ♦ *SMTP Mail Server* check – checks the availability of an SMTP mail server;
- ♦ *SMTP to POP3* check – checks if e-mail service is working properly by sending a test e-mail through an SMTP server and verifying that it has been delivered to the recipient's mailbox;
- ♦ *SNMP GET* check – queries a computer or device using the SNMP (“Simple Network Management Protocol”) protocol, and analyzes the result;
- ♦ *SNMP Trap Receive* check – receives SNMP traps from various machines/devices, and analyzes the message;
- ♦ *TCP/IP* check – checks if a connection can be established on a particular TCP port;

Windows-related checks:

- ♦ *Anti-Virus/Anti-Spam* check – checks status and version of anti-virus software on a workstation or server;
- ♦ *CPU usage* check – monitors CPU usage of processor(s) on a Windows platform. If the load reaches a certain level (for instance: 80%), an alert is generated;
- ♦ *Directory* check – monitors a directory, for instance a user's Home Directory or a common Department Folder;
- ♦ *Disk Drive* check – monitors a physical disk drive on a workstation or server running a Windows Operating System;
- ♦ *Disk Space* check – checks the disk space; an alert is fired when a minimum (or maximum) is exceeded;
- ♦ *Event Log* check – checks for certain events in the Windows Event Log;
- ♦ *File* check – checks if a file exists on a server. It can also check the size of the file and look for specific patterns in the file;
- ♦ *Memory* check – monitors various memory counters of a Windows computer;
- ♦ *Microsoft Exchange* check – monitors the status of an MS Exchange Server (2007/2003/2000/5.x); also monitors the most important MS Exchange performance counters;
- ♦ *Microsoft ISA Server* check – monitors the status of the caching component and/or firewall component of an ISA Server (2006/2004/2000);
- ♦ *Microsoft Message Queue (MSMQ)* check – monitors a Microsoft Message Queue;
- ♦ *Microsoft SharePoint Server* check – monitors the status of an MS SharePoint Server (2007/2003); also monitors the most important MS SharePoint performance counters;
- ♦ *Printer* check – checks a printer for availability by checking status information;
- ♦ *Process* check – checks a process to see if it is running. It can check the memory usage of a process, and count the number of identical processes running. It can also check for any process consuming too much memory;
- ♦ *Scheduled Task* check - checks if a scheduled task has completed successfully or not;
- ♦ *Service* check – checks if a service is running on a server;
- ♦ *User/groups* check – checks groups and group membership;
- ♦ *VBScript* custom check –define your own custom VBScript checks. It should return True for success or False for an error. You can include WMI (Windows Management Interface) and ADSI to add a broad range of system checks.

Environmental checks:

- ♦ *Door* check – environmental check to monitor a door; this requires a Sensatronics Senturion device;
- ♦ *Humidity* check – environmental check to monitor humidity; this requires a Sensatronics environmental monitoring device (e.g. Sensatronics EM1, Sensatronics Senturion);

- ♦ *Power* check – environmental check to monitor power. Requires a Sensatronics Senturion device;
- ♦ *Resistance* check – environmental check to monitor resistance; this requires a Sensatronics Senturion device;
- ♦ *Switch (NC)* check – environmental check to monitor a switch (NC); this requires a Sensatronics Senturion device;
- ♦ *Switch (NO)* check – environmental check to monitor a switch (NO); this requires a Sensatronics Senturion device;
- ♦ *Temperature* check – environmental check to monitor temperature. This requires a Sensatronics environmental monitoring device (e.g. Sensatronics EM1, Sensatronics Senturion);
- ♦ *Wetness* check – environmental check to detect water leaks. This requires a Sensatronics environmental monitoring device (e.g. Sensatronics EM1, Sensatronics Senturion).

Database checks:

- ♦ *Database Query* check – ActiveXperts Network Monitor uses OLE DB (also known as ADO) to check availability of any OLE DB compliant database, including Microsoft SQL, MS Access, Oracle, Paradox and more. You can enter a database query and check the result of the query to determine the result of the check;
- ♦ *ODBC Database* check – checks the availability of a database. Most major database systems support ODBC;
- ♦ *Oracle Database* check – checks for availability of Oracle database by through the SQLNET interface;

Linux/Unix checks:

- ♦ *RSH* check – checks a Linux/ Unix server by executing remote shell scripts (unsecure) and processing StdErr and/or StdOut;
- ♦ *SSH* check – checks a Linux/ Unix server by executing remote shell scripts (secure) and processing StdErr and/or StdOut;

Miscellaneous checks:

- ♦ *Serial Device* check – checks a device connected via a serial COM port.

Add new functionality to the product by writing your own VBScript routines. This way, you can monitor almost every piece of hardware, network protocol, software, and so on. Also, VBScript allows you to include techniques like WMI (Windows Management Interface) and ADSI (Active Directory Service Interfaces).

1.4. Custom Monitoring Checks

ActiveXperts Network Monitor allows you to extend the set of built-in check routines by writing your own check routines.

ActiveXperts uses VBScript for custom checks, because of its wide acceptance and its support for ActiveX technologies. ActiveXperts Network Monitor can process up to 16 VBScript scripts simultaneously (multi-threaded).

The Network Monitor engine uses the Visual Basic Scripting Engine that is part of the Windows Operating System.

By using ActiveX controls, WMI and ADSI, you can write virtually any check yourself. Use the following guidelines when writing a new check:

- ♦ The routine must be a Function, not a Sub;
- ♦ The Function must return True (-1), False (0) or Unknown (1);

- ♦ Set the SYSDATA system variable to the value used in the check. For instance, in a CPU check you can assign the actual CPU value to SYSDATA, so it will be displayed by the Manager application, and is also written to the Log file and report database;
- ♦ Set the SYSEXPLANATION system variable to specify a detailed result; this result is displayed by the Manager application, and is also written to the Log file and report database;
- ♦ All variables must be 'dimmed'.

To monitor Linux and Unix computers, you can make use of custom shell scripts. The shell scripts must be located on the Linux/Unix machine, and should output the result of a check using the following output format:

```
[SUCCESS | ERROR | UNCERTAIN]: { <explanation> } { DATA:<value>}
```

For example:

```
Success: Disk space is more than 30 GB Data:45
```

This indicates that the check failed

Another example:

```
Uncertain: Unable to determine disk space
```

This indicates that the check was successful. '45' indicates the current disk space, and is displayed in the 'Data' column in the Manager application.

1.5. Notifications

There are two situations in which notifications are sent to the system administrators:

- ♦ In case of a Failure;
- ♦ In case of a Recovery.

You can configure the following types of notifications:

- ♦ E-mail notification – Send e-mail messages to the system administrators. A SMTP compliant mail server is required on the LAN/WAN network. SMTP authentication is supported. A secondary mail server is supported, in case the primary mail server is not available;
- ♦ SMS messages – Send alpha-numeric SMS messages, either via a GSM modem connected to the server (Bluetooth/Serial/Infrared) or via an SMPP provider (requires ActiveXperts SMS Messaging Server);
- ♦ SNMP Trap notifications – Send SNMP v1 and SNMP v2c trap notifications to a (remote) network manager. It supports different data types, including strings, integers, IP addresses, time ticks and OID's (object identifiers);
- ♦ Pager messages – Send numeric Pager messages to (mobile) phones or numeric pagers using a Hayes compatible modem. Send alpha-numeric Pager messages using an SNPP provider;
- ♦ Network notifications – Send Network Popup notifications, based on NetBIOS user/computer names;

For each notification type, there's an Address Book. The Address Book organizes recipients in groups; these groups can be used in all monitoring checks, so you don't need to define a recipient list for each check.

For each notification type (except SNMP Trap) you can define Message Template. A Message Template defines the body of a notification message (E-mail, SMS, NetBIOS). The message template contains plain text, and includes variables like: `DATE`, `TIME`, `DISPLAYNAME`, `RESULT` and more (See also Appendix C: "Notification Variables"). These variables are substituted by the Network Monitor Engine at runtime (i.e. when the message is sent out).

Notifications can be repetitive. This means that you can configure a notification to be sent out every *x* minutes after a server/device went down.

1.6. Actions

Actions work in the same way as notifications: they can be triggered upon a critical condition (Failure) or upon Recovery. You can configure the following actions:

- ♦ Execution of a Windows program (executable, batch job or VBScript program);
- ♦ Restart of a Windows service (or multiple services);
- ♦ Reboot of a Windows server or workstation.

Actions can be repetitive, i.e. you can trigger an action every *x* minutes after a server/device went down. You can pass credentials (login and password) for the Restart and Reboot actions; this makes sense if the service account, used for the ActiveXperts Network Monitor service – has no administrative rights on the remote computer.

For batch programs, executables and VBScript programs, you can use parameters like: `DATE`, `TIME`, `DISPLAYNAME`, `RESULT` and more (See also Appendix C: “Notification Variables”). These variables are substituted by the Network Monitor Engine at runtime.

1.7. Errors, Failures and Recovery

A Monitoring Check is always in one of the following states:

- ♦ OK;
- ♦ Error;
- ♦ Failure;
- ♦ Maintenance;
- ♦ Failure by Dependee;
- ♦ On Hold;
- ♦ Not Monitored;
- ♦ Uncertain.

There's a difference between an error, a failure, a failure during maintenance and a failure by dependency:

▼ 'OK' State

The check meets all the conditions. The corresponding computer/device is working fine.

▼ 'Error' State

If a check doesn't match the conditions as defined by the system operator for a while, it's considered as an **Error**. Think of an ICMP check for server 'www.activexperts.com'. Sometimes, the ping will fail (for instance once a week), because a router on the internet has a hick-up. You don't want to ring all bells and whistles in this situation. So, the check is in the **Error** state. But when this error happens a couple a times in a row, it's considered as a **Failure**.

▼ 'Failure' State

A **Failure** is the occurrence of one or more **Errors** in a row. The number of errors (let's say *x*, the so called threshold) is configurable. After *x* errors in a row, it is called a **Failure**. Only on failure, notifications are sent out and actions are triggered.

For instance, with an 'ICMP Ping' check that has the threshold set to 5, a failure notification will be sent after 5 consecutive error pings.

▼ 'Maintenance' State

If the result of a check is not successful during a Maintenance period, it won't be considered as a regular **Error** or **Failure**. Instead, the result will be: **Maintenance**. This indicates that the negative result is caused by maintenance on servers, devices or network. No notifications will be sent and no actions will be triggered.

▼ 'Failure by Dependee' State

If a check fails as a result of another failed server, and there is a dependency relation between these checks, it will not be reported as a regular failure; no notifications will be sent and no actions will be taken.

Imagine you have a server 'S1' on a remote location, and there's router 'R' connecting your LAN with the remote location, and you have ICMP checks for both 'S1' and 'R'.

By making 'S1' dependent of 'R', a failure of 'R' will only result in notifications for 'R', not for 'S'. Dependencies can be configured from the **Dependency command** in the **Tools menu**.

▼ 'On Hold' State

You can put a check 'On Hold'. This means, that the check will not be monitored as long as the check remains 'On Hold'.

▼ 'Not Monitored' State

When a check cannot be processed by the engine, the state is set to **Not Monitored**. Think of a monitoring check based on the SNMP check, but the Network Monitor Engine doesn't have the SNMP service installed. It cannot process the check and will set the result to **Not Monitored**.

▼ 'Uncertain' State

When the result of a check cannot be determined by the Engine, the state is set to **Uncertain**. Think of a Disk Space monitoring check, monitoring free disk space on a file server. If the file server becomes totally unavailable, the Network Monitor Engine cannot determine the Disk Space. In this situation, the result is set to **Uncertain**.

Note: You can change the way Network Monitor handles 'Uncertain' events. By default, all checks which results cannot be determined are set to **Uncertain**. You can configure not to use the 'Uncertain' state, and set each undetermined result to either **Success** or **Error**.

▼ About Recovery

When a server leaves the Failure state and enters the Success state, we're talking about 'Recovery'. 'Recovery' itself is not a state; however, in this situation, Notifications can be sent and Actions can be triggered. This can be useful for Administrators and Operators, so they know that an Action was successful.

1.8. Maintenance Schedules

In most companies, system maintenance is done on specific time intervals. During maintenance, some servers or services will not be available to users. For instance, during backup hours, some services/daemons will be down to avoid open files, mail servers will be stopped, and so on.

In these situations, the Network Monitor Engine will not send alerts or trigger actions in case of a failed check. To accomplish this, you can define Maintenance Schedules. During these periods, no actions/notifications will be triggered in case of a failure.

Maintenance Schedules can be configured globally (for all monitoring checks) or at the Monitoring Check level. You can define multiple maintenance schedules.

2. Installing ActiveXperts Network Monitor

2.1. Software components

The central monitoring service runs on a (dedicated) Windows 2008/Vista/2003/XP/2000 computer; it monitors computers/devices in your LAN, WAN or even outside your enterprise. No additional software is required on the monitored servers.

The graphical Manager application is running on the operators desktop PC; it connects to the central monitoring service, and allows you to make changes to the configurations, and view the results.

▼ Network Monitor Engine

The ActiveXperts Network Monitor Engine is a Windows Service (`AXSNMSVC.EXE`), and is the actual monitoring program. It polls the computers/devices in your LAN/WAN for availability at specific time intervals. This service is multithreading, allowing the service to monitor many computers/devices simultaneously.

The service is responsible for notification, actions, recovery, logging, and so on.

Note: ActiveXperts Network Monitor doesn't require agent software on the servers you monitor; the service only uses protocols and application layers of the Operating System to do its job.

▼ Network Monitor Manager

The ActiveXperts Network Monitor Manager application (`AXSNMAPP.EXE`) is used to view the status of your network and to make changes to the configuration.

You can install the Manager application on any workstation/server in your LAN/WAN.

The Manager application makes a connection to the central ActiveXperts Network Monitor Service, to write configuration information, and to read monitoring information.

The Manager application can be installed on any Windows 2000 or higher computer (workstation or server).

▼ Report Generator

The ActiveXperts Network Monitor Report Generator can be used to create new reports. There are two versions: a graphical version (`AXRGGUI.EXE`) to create reports using a wizard, and a command line version (`AXRGCMD.EXE`) to create reports from the command line or from the Task Scheduler.

Reports can only be created by using a Report Definition file (`.rep`). Such a definition file describes the properties of a report (like: filters, sorting, layout, output file, etc.).

▼ Report Configurator

The ActiveXperts Network Monitor Report Configurator (AXRGTP.L.EXE) can be used to define new report definition files. A report definition file (.rep) can be used as an input file to the Report Generator.

▼ Web Interface

Collection of XML- and XSL files. An XML file can be opened by the Internet browser. The associated XSL file is used to make-up the XML page so it can be viewed by your Internet Browser.

▼ Web Interface Configurator

The ActiveXperts Network Monitor Web Interface Configurator (AXWEBCFG.EXE) can be used to customize the Web Interface.

▼ Installation Files

The full ActiveXperts Network Monitor package is available on the internet as a one setup file: AMONITOR.EXE.

After you download the file from the internet, you start the setup procedure on the server that you assigned as the monitoring server. This server doesn't have to be a dedicated server. The installation will install the monitoring service, the Manager application and several tools and utilities.

2.2. Installing ActiveXperts Network Monitor

▼ Hardware requirements

The ActiveXperts Network Monitor service only runs on a Windows workstation or server platform, and must meet either of the following requirements:

	Windows 2008	Windows 2003	Windows 2000	Windows Vista	Windows XP Prof.
CPU	1 GHz (x86) or 1.4 GHz (x64)	550 MHz (x86) or 733 MHz (x64)	x86 133MHz or higher	1 GHz 32-bit (x86) or 64-bit (x64)	233 MHz (x86) or 733 MHz (x64)
Memory	1GB or more	256MB	128 MB	512 MB	128 MB
Service Pack	-	SP1	SP4 or higher	-	SP1 or higher
Available Diskspace	1GB	1GB	500 MB	1GB	500 MB

It's recommended to use a server platform for the ActiveXperts Network Monitor Service, because server platforms support more simultaneous network connections. Server platforms are optimized for application services.

Usually, the installation is done only once, on the server that is dedicated as the monitoring server. A wizard will take you through the installation.

▼ Upgrading ActiveXperts Network Monitor from a previous version

Upgrade of ActiveXperts Network Monitor requires un-installation first, followed by a new installation of the software. All configuration files will be preserved during un-installation. However, it is recommended to export the configuration to a save place, before you uninstall the product.

▼ Upgrade – Step-by-Step

Step 1 – Export the Configuration (Recommended, not required)

In the Manager application, choose Export Configuration from the File menu, and export the configuration to a save place.

Step 2 – Run the Setup application

Launch the Setup application (`AMONITOR.EXE`). It will detect a previous installation of ActiveXperts Network Monitor. It will ask to press OK to uninstall the current installation of ActiveXperts Network Monitor. After pressing OK, the software will be uninstalled. The previous configuration files will be preserved.

Step 3 – Install ActiveXperts Network Monitor

Launch the Setup application (`AMONITOR.EXE`) again. Follow the steps described below.

Step 4 – Import a configuration

After the installation has completed, you can import any Network Monitor configuration file, no matter what version of Network Monitor was used to create it.

▼ Installing ActiveXperts Network Monitor

Before you start the installation, you must assign one of your Windows servers in your network as the ActiveXperts Network Monitor Server. This machine will host the Network Monitor Engine (service).

Download the installation file `AMONITOR.EXE` from the internet (<http://www.activexperts.com/download>) and run this program on the server that you assigned as the monitor server.

The following components will be installed on that server:

- ◆ ActiveXperts Network Monitor **Service** – the actual Network Monitor Engine;
- ◆ ActiveXperts Network Monitor **Manager application** – to let system administrator make changes to the configuration and view/analyze results;
- ◆ ActiveXperts Network Monitor **Report Generator** and **Report Configurator** – allows administrators to create/modify report definition files, and to create new reports;
- ◆ ActiveXperts Network Monitor **Web Interface Configurator** – allows administrators to customize the Web Interface;
- ◆ ActiveXperts Network Monitor **Remote Manager Configurator** – allows administrators to configure the Manager application for use on remote workstations.

▼ Installation – Step-by-Step

Step 1 – Welcome Message

This is where the installation begins.

Step 2 – Setup Type

Choose “Network monitor Engine + Management Console” if you want to install the Network Monitor service. The first installation should always be this type of installation.

After the first installation, you can run a “Management Console” installation on network workstations to allow users to view the monitoring results of Network Monitor, or to make changes to the configuration.

Step 3 – Registration information

Here, you can enter your Registration code. If you want to try the software, enter ‘EVALUATION’ as the registration code. You will be able to use the software for 30 days. If you decide to buy after 30 days, you don’t need to re-install; the Manager application allows you to enter the registration code and the software will continue working.

Step 4 – Choose Destination Folder

Choose a destination folder. Setup will copy the service, the Manager application, the Manager Setup files and other components to this location. Please make sure to have approximately 50 megabytes available.

Step 5 – Select Program Folder

Specify a name for the Program folder.

Step 6 – Service Account

The Network Monitor Engine (a Windows service) must run with specific credentials. It’s recommended to provide a Domain Admin or Enterprise Admin account, because it is likely that ActiveXperts Network Monitor needs access to servers in the domain with administrative rights to do its job. However, it’s not mandatory to provide a Domain/Enterprise Admin account; for every monitoring check, alternate credentials can be provided.

Step 7 – Reboot (only for Windows 2000)

If you install the software on a Windows 2000 platform, you may be asked to reboot the computer.

2.3. Installing Management Console on a Workstation

▼ About Installing the Management Console

Use the ActiveXperts Network Monitor Manager application to:

- ◆ Make changes to the configuration;
- ◆ View the monitoring results;
- ◆ Run reports.

The Manager application is already installed by default on the server where the ActiveXperts Network Monitor service runs. So, there's no need to run ActiveXperts Network Monitor Manager installation on the server.

By default, installing ActiveXperts Network Monitor Manager applications on remote computers is prevented for security reasons. To allow the installation of the Manager application on other computer, a share must be created. This share will be used by the remote Manager application to communicate with the Network Monitor Engine.

To define the Share:

- ◆ Start the ActiveXperts Network Monitor Manager application on the computer where the Network Monitor Engine is running;
- ◆ Choose **Manager on Remote Workstations** from the **Tools menu**, and select the **Install Manager on Remote Workstations** tab;
- ◆ A wizard pops up; in this wizard, define a **Share name** and press the **Create Share** button.

Once you have created the share, you're ready to install the Network Monitor Manager on remote PC's.

Simply run the `AMONITOR.EXE` setup program (same installation as used for the server installation) on the workstation, and choose 'Install Management Console on a Desktop PC or Notebook'. The Setup program will now prompt for a share. Enter the share (UNC format) of the central ActiveXperts Network Monitor directory.

To be able to run the Network Monitor Manager application on workstations, Users (operators) need Change (RWX) permissions on the files in the shared directory.

Note: To allow/prevent users in the network from installing/running the Network Monitor Manager, simply use NTFS permissions or Share Permissions. The easiest is to use Share Permissions: simply add/remove RWX permissions to allow/prevent Users or Groups at Share level.

▼ Hardware requirements

The ActiveXperts Network Monitor Manager application runs on Windows 2000 Professional platforms or higher, and must meet either of the following requirements:

	Windows 2008	Windows 2003	Windows 2000	Windows Vista	Windows XP Prof.
CPU	1 GHz (x86) or 1.4 GHz (x64)	550 MHz (x86) or 733 MHz (x64)	x86 133MHz or higher	1 GHz 32-bit (x86) or 64-bit (x64)	233 MHz (x86) or 733 MHz (x64)
Memory	1GB or more	256MB	128 MB	512 MB	128 MB
Service Pack	-	SP1	SP4 or higher	-	SP1 or higher
Available Diskspace	1GB	1GB	500 MB	1GB	500 MB

▼ Installation Step-by-Step

Step 1 – Welcome Message

This is where the installation begins.

Step 2 – Setup Type

Choose 'Install Management Console on a Desktop PC or Notebook'. It will install the Network Monitor Manager, the Report Generator and some utilities on the workstation PC.

Step 3 – Location of the central Network Monitor server

You're prompted for the location of the central Network Monitor Server share. Enter the share, as created on the server machine by the 'Network Monitor Remote Manager Configurator'.

Step 4 – Choose Destination Folder

Choose a destination folder. Setup will copy all client application files to this location. Please be sure to have approximately 5MB available, depending on the type of installation.

Step 5 – Select Program Folder

Specify a name for the Program folder.

Step 6 – Reboot (only for Windows 2000)

If you install the software on a Windows 2000 platform, you may be asked to reboot the computer.

3. Configuring ActiveXperts Network Monitor

3.1. Introduction

The ActiveXperts Network Monitor configuration consists of two parts

- ♦ Monitoring checks – all monitoring checks and monitoring properties;
- ♦ Global configuration data – this data is configured independent from the monitoring checks, and contains global notification settings, address books, default settings, web interface settings, report settings and more.

All configuration data is stored in an MS Access database called: `CONFIG.MDB`. This file is located in the `<INSTALL-DIR>\Configuration\` directory.

Use the **ActiveXperts Network Monitor Manager application** to make configuration changes, to view real-time monitoring information, and to analyze results. The Manager application can be launched from any Win32 platform, or from the machine where the service is running on.

You don't need to restart the service every time you make changes to the configuration. The service will detect configuration changes as they are made, and will reload the configuration.

The ActiveXperts Network Monitor configuration can be imported, exported and cleared at any time. By using the **Export** command, the configuration can be backed up to a save location. By using **Import** command, a configuration can be loaded and set as the current configuration. By using the **Clear** command, you can clear your current configuration and start from scratch. None of the above commands need a restart of the ActiveXperts Network Monitor Service.

3.2. ActiveXperts Network Monitor Manager

To launch the **ActiveXperts Network Monitor Manager**, click **Start**, point to the **ActiveXperts Software** folder, point to the **Network Monitor** folder and click on the **Network Monitor Manager** icon.

▼ Views

The ActiveXperts Network Monitor Manager application window is divided into three views:

- ♦ Folder view (left view) – Checks can be grouped in logical containers called Folders;
- ♦ Checks view (right view) – list of checks that are organized in the selected folder. The checks in the subfolder(s) of the selected folder are also displayed;
- ♦ Activity Log view (bottom view) – shows the activity of the ActiveXperts Network Monitor service.

▼ Permissions

The ActiveXperts Network Monitor Manager application can be run in two different modes:

- ♦ Read-write mode (default) – view results, make reports and make changes to the configuration; Read-write access is required for administrators who install and configure ActiveXperts Network Monitor.








- ♦ Read-only mode – only view results; in Read-only mode, you can't make changes to the configuration. Read-only mode is ideal for people who work at the Help Desk and do first line support.


▼ Assigning permissions

The next chapter discusses how to assign read-write and read-only permissions to users and groups.

▼ State Information and Icons

In the server view, an icon precedes every server entry. Here's a list of all possible state values (with corresponding icons) and their meanings:

-  **OK** – The check meets all the conditions. The corresponding server/device is working fine.
-  **Error** – When a check doesn't meet the conditions as defined by the system operator for a while, it's considered as an Error. For instance, when you configure an ICMP check for web server 'www.activexperts.com', a ping may fail for instance once a day, for example because a router on the internet has a hick-up. You don't want ring all bells and whistles in this situation, because the problem has nothing to do with the actual server. So, the check is in the Error state. Only when the error happens a couple a times in a row, the status is set to Failure.
-  **Failure** – A Failure is the occurrence of 1 or more errors in a row. This error threshold is configurable. Only when the error happens x times in a row, the status is set to Failure. Only then, notifications are sent out and actions are taken. For instance, when you configure an ICMP check, you should configure to let the check fail only after a couple of errors in a row, let's say 5. So, only when 5 errors occur in a row, the result of the check will be: Failure. Only then, Administrators and Operators will be notified of this failure event.
-  **Maintenance** – When the result of a check is not successful during Maintenance hours, it won't be considered as an ordinary Error or Failure. The result will be: Maintenance, to indicate that the negative result is due to the maintenance on computers/devices. No notifications will be sent and no actions will be triggered.
-  **Failure by Dependee** – When a server fails (after a number of errors in a row) as a result of another failed server, and there is a dependency relation between them, it won't be considered as an ordinary failure; no notifications will be sent and no actions will be taken. Suppose you have a server 'S1' on a remote location, and there's router 'R' connecting your LAN with the remote location, and you have ICMP checks for both 'S1' and 'R'. You should make 'S1' dependent of 'R'. In that scenario, when 'R' fails, you won't get actions/notifications from 'S1'.
-  **On Hold** – You can put a check 'On Hold', so it won't be processed by the Network Monitor Engine.
-  **Not Monitored** – Initial state of a check. When the Network Monitor service has just been started, all checks will have status Not Monitored.

 **Uncertain** – When the result of check cannot be determined by the Engine, the state is set to Uncertain. Think of a Disk Space check, monitoring free disk space on a File Server. If the File Server becomes unavailable (for instance because it has completely crashed), the Network Monitor Engine cannot determine the Disk Space. In this situation, the result will be set to Uncertain.


3.3. ActiveXperts Network Monitor Quick Configuration Wizard

The first time you start the ActiveXperts Network Monitor Manager application, the **Quick Configuration Wizard** pops up to collect some basic information, like: your SMTP e-mail server, your e-mail address, and so on. The Quick Configuration Wizard also adds some sample monitoring checks to your configuration.

3.4. Import, Export and Clear configuration settings

▼ Import configuration settings

To import a previously saved configuration, use the Import function. Note that the current configuration will be overwritten.

To quickly import a configuration, click **Import**  on the toolbar.


To import a configuration:

- ◆ On the **File menu**, choose **Import Configuration**;
- ◆ Select the **version** of the import configuration file, and click **Next**;
- ◆ In the **File name** box, enter a name of a previously exported configuration file;
- ◆ Click **Finish** to finish the import.

Note: It is possible to Import a configuration file that was created on another computer.

▼ Export configuration settings

It's a good practice to make a backup after major configuration changes. The 'Export Configuration' function exports all of the configuration settings. This means: all global configuration settings (like mail server, default scan time, etc.) as well as all monitoring checks.

To quickly export a configuration, click **Export**  on the toolbar.

To export a configuration:

- ◆ On the **File menu**, choose **Export Configuration**;
- ◆ In the **File name** box, enter a name for the new export configuration file;
- ◆ Click **Save**.

Note: The Auto Backup feature automatically exports the configuration periodically. Auto Backup can be configured from the **Auto Backup tab** of the **Options dialog**.

▼ New configuration

The New Configuration function clears the existing configuration and creates a new one. The ActiveXperts Network Monitor Manager will ask you to save the current configuration before you clear it.

To quickly create a new configuration, click **New Configuration**  on the toolbar.

To create a new configuration:

- ◆ On the **File menu**, click **New Configuration**;
- ◆ The program will ask if you want to export the current configuration;
- ◆ After the optional export, it asks you if you're sure to create a new configuration. Press **Yes**.

3.5. Renaming computers

▼ Renaming the ActiveXperts Network Monitor Engine computer

To rename the computer where the ActiveXperts Network Monitor Engine is running on, you must take the following steps:

- ◆ Export the configuration to a save place, using the Manager application;
- ◆ Stop the Network Monitor Engine;
- ◆ Quit the Network Monitor Manager application. Also quit Network Monitor Manager applications on remote workstations (if any);
- ◆ Change the following registry entries:
`HKLM\Software\ActiveXperts\Network Monitor\Engine0`
`HKLM\Software\ActiveXperts\Network Monitor\Engine0Root`
- ◆ Start the Network Monitor Engine;
- ◆ Import the configuration file. The Import Wizard will detect that the configuration was previously used on a machine with a different name, and will ask you to confirm so that the configuration will be converted.
- ◆ On other PCs in the network that have the Manager application installed, make changes to these two registry entries:
`HKLM\Software\ActiveXperts\Network Monitor\Engine0`
`HKLM\Software\ActiveXperts\Network Monitor\Engine0Root`

▼ Renaming the ActiveXperts Network Monitor Manager computer

You can change the name of the computer where the Manager application is running. This will not affect the ActiveXperts Network Monitor Manager installation.

3.6. Configuring Monitoring Checks

To add a new monitoring check, click **New Monitoring Check**  on the toolbar.

To configure an existing monitoring check, double click on the particular check entry in the Manager application, or right-click on the selected check and choose 'Properties'.

Most important configuration items of a Monitoring Check are:


- ◆ **Check What** – the type of check that is performed on a specific network device, server or workstation;

- ◆ **Display Name** – the name of the check to be displayed by the Manager application. The display name is also used in log files and reports to refer to this Monitoring Check. The display name can be any user friendly name.
- ◆ **Check every / Schedule this Check** – specifies how frequent a check will be scanned. You can set it to scan it at a specific date and time, or to scan it frequently with a specific interval.
- ◆ **Check fails after x errors in a row** – specifies the number of consecutive errors that must occur before a check will be considered as 'Failed'; by default, a check will be considered as 'Failed' after 3 consecutive errors. This option only applies to a check that is not scheduled.

The configuration of checks is discussed in detail in Chapter 4: "Managing Monitoring Checks".

3.7. Options

Options are properties that are global for all monitoring checks.

You can configure these from the **Tools menu**, by selecting the **Options item**, or by pressing  on the toolbar.

▼ Defaults

'Defaults' apply to new Monitoring Checks. Default values can be defined in the Options dialog:

- ◆ On the **Tools menu**, click **Options**;
- ◆ Select the **Defaults tab**.

The following default values can be configured:

- ◆ **Check every x seconds/minutes/hours/days** – specifies how often a monitoring check routine will be scan for a *new* monitoring check; Initial default value: 30 seconds;
- ◆ **Check fails after x errors in a row (error threshold)** – specifies the number of consecutive errors that must occur before a new monitoring check will be considered as Failed; Initial default value: 3.

Default values only apply to new checks; they do not affect existing monitoring checks. However, you can apply the default values to all monitoring checks by pressing the **Copy/Paste Special** from the **Edit menu**.

▼ Logging

To configure logging, select the **Options item** from the **Tools menu**, and select the **Logging tab**; ActiveXperts Network Monitor maintains its own log files. By default, logging is enabled. To enable/disable logging:

- ◆ Select/deselect the **Enable Logging check box**.

By default, ActiveXperts Network Monitor only logs status changes. You may want to log all events. This can be achieved in the following way:

- ◆ Select/deselect the **Log all monitoring activities**.

ActiveXperts Network Monitor supports the following log file formats:

- ◆ Plain Text log files, delimited by a configurable separator. This is the default log format.

Logging information is written to the following directory by default:

`<installation directory>\Logs`

- ♦ OLE DB compliant databases, including MS Access and MS SQL. OLE DB is also known as ADO.

On www.activexperts.com/support/activmonitor/online/netmonlogging/ (online Network Monitor Logging Guidelines) you can find information about configuring OLE DB (ADO) logging. The guidelines also explain how to migrate logging from MS Access to MS SQL, and how to troubleshoot OLE DB logging.

▼ Server Credentials

By default, Network Monitor uses the Service Account credentials to monitor remote Windows servers. However, if these credentials do not have administrative permissions on a remote Windows server (for instance because the remote machine is member of another domain, or because the server is a standalone server) you can specify alternate credentials. These alternate credentials are administrated globally, and can be used in any Windows check.

▼ Date and Time

Network Monitor does not use Windows' Date/Time settings for displaying information, because results can be viewed by non-Windows users (Web interface, reports, etc.). Therefore, you can set Date/Time settings; these settings are stored in the configuration database, and will be used by all Manager applications, Web Views, Reports, etc..

To configure Date/Time settings:

- ♦ On the **Tools menu**, click **Options** and select the **Date and Time** tab;
- ♦ Select your preferred Time format and Date format.


▼ Auto Backup Settings

Automatic Backup is enabled by default, and will backup the configuration file and all VBScript programs to a fixed network location automatically, periodically. For more details regarding Backup and Restore, please read chapter 3.17: "Backup and Restore".

3.8. Notifications

Notifications are sent in two situations:

- ♦ When a Monitoring Check fails – After a configurable number of errors (error threshold), the check is set to Failed. Probably you want to send notifications to the system operator via the SMS or e-mail to notify him that the server/device is down;
By default, only one notification is sent after a failure; if you want to be notified regularly after a failure, it can be configured by pressing the **Advanced** button in the **Monitoring Check Properties** tab;
- ♦ When a Monitoring Check is recovered from the Failed status – ActiveXperts Network Monitor has the ability to repair a computer/device. It can be useful to send an alert to the operator to tell him that the previous error is no longer there.

Notification Settings are software settings that are global for all monitoring checks. You can configure them from the **Tools menu**, by selecting the **Notification Setup** item, or by pressing  on the toolbar.

For all notification types - except pager notifications and SNMP traps - you can use an **Address Book**. In the Address Book, you can organize notification recipients in groups. Groups can be used in any check. But you can still define a custom list of recipients for individual checks.

The following notification types are supported by ActiveXperts Network Monitor:

- ◆ E-mail notifications;
- ◆ Network notifications;
- ◆ Alpha-numeric SMS notifications;
- ◆ Numeric Pager notifications;
- ◆ Alpha-numeric Pager notifications;
- ◆ SNMP Trap notifications.

▼ Default notification settings for new Monitoring Checks

Default notification settings apply to new Monitoring Checks. These values can be defined in the Notifications dialog:

- ◆ On the **Tools menu**, click **Notifications**;
- ◆ Select the **Defaults tab**.

The following notification defaults can be configured:

- ◆ **Send E-mail notification when server goes offline** – this value indicates whether an e-mail notification should be sent when a check fails;
- ◆ **Send Email notification when server goes online** – this value indicates whether an e-mail notification should be sent when a check is successful after a failure;
- ◆ **Send SMS notification when server goes offline** – this value indicates whether an SMS notification should be sent when a check fails;
- ◆ **Send SMS notification when server goes online** – this value indicates whether an SMS notification should be sent when a check is successful after a failure;
- ◆ **Send Pager notification when server goes offline** – this value indicates whether a Pager notification should be sent when a check fails;
- ◆ **Send Pager notification when server goes online** – this value indicates whether a Pager notification should be sent when a check is successful after a failure;
- ◆ **Send SNMP Trap notification when server goes offline** – this value indicates whether an SNMP Trap notification should be sent when a check fails;
- ◆ **Send SNMP Trap notification when server goes online** – this value indicates whether an SNMP Trap notification should be sent when a check is successful after a failure;
- ◆ **Send Network notification when server goes offline** – this value indicates whether a network notification should be sent when a check fails;
- ◆ **Send Network notification when server goes online** – this value indicates whether a network notification should be sent when a check is successful after a failure;
- ◆ **Notification Frequency Defaults** – specifies how often a notification (e-mail, SMS and so on) should be sent after a failure. By default, a notification is sent only once after failure; however, you can configure to notify every x minutes after failure;
- ◆ **Action Frequency Defaults** – specifies how often actions (restart service, restart computer, run program, and so on) should be triggered after failure. By default, an action is triggered only once after failure; however, you can configure to trigger an action every x minutes after failure.

3.9. E-mail Notifications


To use SMTP e-mail notifications, the ActiveXperts Network Monitor service must have access to a SMTP server to send out e-mails. It can be any SMTP compliant mail server. You don't need IIS to be installed.

Note: ActiveXperts Network Monitor doesn't require IIS or an IIS SMTP connector; it communicates directly with the SMTP server using the SMTP protocol.

ActiveXperts Network Monitor is compliant with SMTP servers that require SMTP authentication, like Microsoft Exchange. SMTP AUTH is the protocol that is used to verify that you are one of the users of the SMTP server. ActiveXperts Network Monitor is RFC 821 and RFC 822 SMTP AUTH compliant.

It also supports multiple character sets, including English (ISO-8859-1), Chinese (big5) and Japanese (ISO-2202-JP).

▼ E-mail Notification Settings - General

To quickly configure general e-mail notification settings, click **Notification Setup**  on the toolbar.

To configure general e-mail notification settings:

- ◆ On the **Tools** menu, click **Notification Setup** and select the **E-mail** tab;
- ◆ Enable the **Enable E-mail Notifications checkbox** to enable e-mail notifications;
- ◆ The **SMTP mail server** can be an IP address (like 10.0.0.1), a host name (like mail.mydomain.com) or a NetBIOS name (like EXCHANGE01); this is the server that will send out the actual notification messages to the recipients;
- ◆ If your SMTP server requires authentication, click the **authentication checkbox** and provide a **logon** and **password**;
- ◆ Provide **Sender E-mail Address** (required) and **Sender's Display Name** (optional). The recipient will see this name/address as the sender, and all replies will be delivered to this mail account;
- ◆ Use the **E-mail Address Book** to organize e-mail recipients in groups. The Address Book can be used for all checks. The E-mail Address Book makes configuration easier, because you don't have to configure a separate list of recipients for each monitoring check; however, it is still possible to configure a separate list of recipient for any check;
- ◆ Click on **Format Message** to edit the e-mail template and to enable/disable RTF (HTML) formatting. In this dialog, you can also set the preferred character set: English (ISO-8859-1), Chinese (big5) or Japanese (ISO-2202-JP). Enable **RTF (HTML) formatting** to support HTML tags. If you switch on RTF formatting, you must use the `
` tag (or an alternative tag) to insert new lines.
- ◆ Click on **Secondary Server** to specify a fallback server. The secondary server is only used if the primary SMTP mail server is down while attempting to send out an SMTP notification.

To test the E-mail Notification Settings, use the **Test SMTP Server** button. It will send a request the Network Monitor Engine to send an E-mail message using the given settings.

Message Templates are discussed in Chapter 3.14: "Message Templates".

Note: Be aware of e-mail clients that do not have Rich Text enabled for security reasons. For instance, Windows 2003 has the 'Read all messages in plain text' option switched on in Outlook Express by default, so that incoming Rich Text messages may look garbled.

▼ Using E-mail Notifications in a check


For each check, you can make the following configuration settings:

- ◆ **Notify when check fails** – when the check is set to Failure, a message is being sent. Default: On;
- ◆ **Notify when a check recovers from a failed state** – when the check turns from Failure to Success, a message is being sent. Default: Off;
- ◆ For both Success and Failure status changes, you use the **Address Book** recipient groups, or use a custom recipient list.

3.10. Network Notifications

Network Notifications are the well-known ‘Net Send’ (or ‘NetPopup’) messages over the network. Only machines that support NetBIOS (like Windows and OS2) can send/receive these messages. NetBIOS messages can be sent to users and/or computers.

▼ Network Notification Settings - General

To quickly configure general network notification settings, click **Notification Setup**  on the toolbar.

To configure general network notification settings:

- ◆ On the **Tools** menu, click **Notification Setup** and select the **Network Popup** tab;
- ◆ Enable the **Enable Network Popup Notifications** checkbox to enable network notifications;
- ◆ Use the **Network Popup Address Book** to organize NETBIOS recipients in groups. The Address Book can be used for all checks. The Address Book makes configuration easier, because you don’t have to configure a separate list of recipients for each monitoring check; however, it is still possible to configure a separate list of recipient for any check;
- ◆ Click on **Format Message** to edit the network message template. Message Templates are discussed in Chapter 3.14: “Message Templates”.

To test the Network Notification Settings, use the **Send Test Message** button. It will send a request the Network Monitor Engine to send an network popup message using the given settings.

▼ Using Network Notifications in a check

For each check, you can make the following configuration settings:


- ◆ **Notify when check fails** – when the check is set to Failure, a message is being sent. Default: On;
- ◆ **Notify when a check recovers from a failed state** – when the check turns from Failure to Success, a message is being sent. Default: Off;
- ◆ For both Success and Failure status changes, you use the **Address Book** recipient groups, or use a custom recipient list.

3.11. SMS Notifications

ActiveXperts Network Monitor supports alpha-numeric SMS messaging in two ways:

- ◆ Through a GSM Modem (or GSM phone), connected to the Network Monitor server by serial cable, Infrared or BlueTooth;
- ◆ Via an SMPP SMSC service center. This requires [ActiveXperts SMS Messaging Server](#) on one of your network computers (or on the same machine as ActiveXperts Network Monitor).

▼ SMS Notification Settings - General

To quickly configure general SMS notification settings, click **Notification Setup**  on the toolbar. To configure general SMS notification settings:

- ◆ On the **Tools** menu, click **Notification Setup** and select the **SMS** tab;
- ◆ Enable the **Enable SMS Notifications** checkbox to enable SMS notifications;
- ◆ Choose **Use GSM Modem...** to send SMS notifications via a GSM modem, or choose **Use ActiveXperts SMS Messaging Server** to forward SMS notification requests to [ActiveXperts SMS Messaging Server](#);
- ◆ Click on the **Format Message** button to edit the SMS template. Message Templates are discussed in Chapter 3.14: “Message Templates”.

▼ SMS Notification Settings – GSM Modem (GSM Phone)

In the GSM Modem setup dialog, you must select the Windows telephony device (recommended) or a physical COM port (directly) that is used to connect to the physical GSM modem. As soon as you select the device from the list, the Network Monitor Manager tries to detect the device connected to the Network Monitor server. If a GSM modem cannot be detected, a log file is provided for troubleshooting purposes.

Use the **Advanced Settings** button to configure advanced communication settings.

▼ SMS Notification Settings – ActiveXperts SMS Messaging Server

ActiveXperts SMS Messaging Server is an SMS messaging framework to enable sending, receiving and processing of SMS messages. You can relay SMS notifications from any application (including Network Monitor) to the SMS Messaging Server.

With ActiveXperts SMS Messaging Server, you can benefit from the product’s SMPP support. SMPP is the fastest and most reliable way of sending bulk SMS messages.

To relay Network Monitor SMS notifications to ActiveXperts SMS Messaging Server, you must install the [ActiveXperts SMS Messaging Server Client Tools](#) on the server that has the Network Monitor service running. Once installed, you can select an SMPP channel (or a GSM channel).

▼ SMS Recipient Number

The SMS recipient number must be in International Number Format: the SMS number, prefixed by the international dialing number and the '+' character. The use of the '+' character is required. For example: +4412345678

▼ Using SMS Notifications in a check

For each check, you can make the following configuration settings:

- ◆ **Notify when check fails** – when the check is set to Failure, a message is being sent.
Default: On;
- ◆ **Notify when a check recovers from a failed state** – when the check turns from Failure to Success, a message is being sent. Default: Off;
- ◆ For both Success and Failure status changes, you use the **Address Book** recipient groups, or use a custom recipient list.


Note: To log all modem operations, you must enter a valid file name in the following registry entry:
 THKLM\Software\ActiveXperts\Network Monitor\Server\Trace\NotifySms

3.12. Pager Notifications

ActiveXperts Network Monitor supports numeric DTMF Paging (using a Hayes compatible modem) and alpha-numeric paging (using an SNPP provider).

The modem must be connected to the server where the Network Monitor Engine is running. When there's a failure, ActiveXperts Network Monitor uses the modem to dial-out to the Pager recipients.

▼ Pager Notification Settings - General

To quickly configure general Paging notification settings, click **Notification Setup**  on the toolbar.

To configure general Pager notification settings:

- ◆ On the **Tools menu**, click **Notification Setup** and select the **Pager tab**;
- ◆ Enable the **Enable Pager Notifications checkbox** to enable pager notifications;
- ◆ Choose **Use alpha-numeric paging...** to send alpha-numeric pager messages using an SNPP provider, or choose **Use numeric DTMF paging...** to send numeric DTMF pager messages using a standard Hayes compatible modem.

▼ Pager Notification Settings – alpha-numeric SNPP paging

In the Pager/SNPP setting dialog:

- ◆ Enter the **Host (host name or IP address)** of your SNPP paging provider. Enter the IP **port** used to connect to your SNPP provider (default: 444);
- ◆ If your SNPP provider requires a password, enable the **Password required option** and provide a valid **password**.
- ◆ In the **Time-out field**, enter the time-out (in millisecond) used to connect to the SNPP provider.

▼ Pager Notification Settings – numeric DTMF paging using a modem

In the Pager/DTMF setting dialog:

- ◆ Select a **Modem** from the list. The list is inherited from the list of Telephone Devices of the operating system (configured in the Control Panel on the system where the Network Monitor

Engine is installed). If there is no modem driver installed for your device, you can also select a direct com port. Use the **Test Pager Settings** button to test the configuration;

Note: A Pager recipient can only consist of the following characters:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, +, -, *, #, @, a, b, c, d, A, B, C, D, w, W

▼ Using Pager Notifications in a check

For each check, you can make the following configuration settings:


- ◆ **Notify when check fails** – when the check is set to Failure, a message is being sent.
Default: On;
- ◆ **Notify when a check recovers from a failed state** – when the check turns from Failure to Success, a message is being sent. Default: Off;
- ◆ For both Success and Failure status changes, you use the **Address Book** recipient groups, or use a custom recipient list.

Note: To log all Pager operations, you can enter a valid file name in the following registry entry:
HKLM\Software\ActiveXperts\Network Monitor\NotifyPager

3.13. SNMP Trap Notifications

ActiveXperts Network Monitor supports SNMPv1 and SNMPv2c Trap notifications.

▼ SNMP Trap Notification Settings - General

To quickly configure general SNMP Trap notification settings, click **Notification Setup**  on the toolbar.

To configure general SNMP Trap notification settings:

- ◆ On the **Tools** menu, click **Notification Setup** and select the **SNMP Traps** tab;
- ◆ You can now configure a list of SNMP Traps. Usually, you will need just one trap to send out to a network management station, but you can define multiple traps.
Press the **Add Trap** button to add a trap to the list; press the **Edit Trap** button to edit the parameters of a specific trap, and press the **Remove Trap** button to remove a trap from the list.
- ◆ When you use the Add Trap button or the Edit Trap button, you can configure the parameters of a single trap. These parameters are described below.

▼ SNMP Trap Parameters

A trap consists of the following parameters:

- ◆ **Agent** – the host name or IP address of the (remote) SNMP network management station;
- ◆ **Port** – the port used for sending SNMP traps; default: 162;
- ◆ **Community** – the community of SNMP devices. Default: **public**;
- ◆ **Protocol Version** – when you want to send a trap notification to an SNMPv1 compliant network management station, you must select **SNMP v1**. If the network management station runs **SNMP v2c** or higher, you must select **SNMP v2c**. Default: **SNMP v2c**;

- ◆ **OID** – the Object Identifier; Network Monitor accepts numeric and alpha-numeric OID's, for instance: `system.sysName.0`, or `1.3.6.1.2.1.1.5.0`;
- ◆ **OID Data Type** – this field indicates the type of data that is sent to the (remote) network management station. Network Monitor supports the following data types: strings, integers, IP addresses, time ticks, counter types, OID's and some other, less frequently used types;
- ◆ **OID Value** – the actual value that is sent over the network. You can include notification variables, like `<%DISPLAYNAME%>`, `<%TIME%>`, or `<%SERVER%>`. For a complete list of notification variables, see also Appendix C: "Notification Variables";
- ◆ **Generic Trap** – this optional field is only used with SNMP v1.

▼ Using SNMP Trap Notifications in a check

For each monitoring check, you can configure the following settings:

- ◆ **Notify when check fails** – when the check fails, a message is being sent. Default: **On**;
- ◆ **Notify when check recovers from a failed state** – when the check reverts to 'success', a message is being sent. Default: **Off**;
- ◆ For both Online and Offline status changes, you can choose to use **Global SNMP Trap List** as defined in the General SNMP Trap Notification Settings, or use a **Custom SNMP Trap List**.

3.14. Message Templates

A notification message can be customized. Use the **Format Message** button in the appropriate general notification tab of the **Notification Setup** dialog from the **Tools menu**. Each notification type has its own message template.

Inside a message template, you can use system variables. These variables are substituted each time the message is sent out. System variables must be enclosed between `<%` and `%>` strings, for example: `<% DATE %>`. See also Appendix C: "Notification Variables" for a complete list of Notification Variables.

▼ Message Template Example

Example of a message template:

```
Message from ActiveXperts Network Monitor on <% SERVER %>, <% DATE %> <%TIME %>:
Item:      <% DISPLAYNAME %>
Result:    <% RESULT %>
Explanation:<% EXPLANATION %>
```

Note: Using newlines in SMS Message Templates is NOT recommended. Many GSM phones don't know how to handle newlines and will display bad characters.

3.15. Maintenance

To avoid notifications and actions during maintenance hours, you can configure maintenance schedules. All failures that happen during these schedules won't be notified, and no actions will be triggered.

The maintenance schedules can be configured as **Every Day of the Week**, or as **On This Date**.

To configure maintenance schedules:

- ◆ On the **Tools menu**, click **Maintenance**; here, you see the list of configured schedules. You can define multiple schedules;
- ◆ To add a new schedule, choose either **Day of Week** or **This Date**.
In case of 'This Date', provide start date and time, and provide the number of hours the computer and devices will be unavailable;
In case of 'Day of Week', provide the days of the week that the computers and devices will be unavailable; also provide a start time, and provide the number of hours the servers will be unavailable.
- ◆ Press the **Add button** to add the new schedule to the **Maintenance Schedules list**.

By default, the maintenance schedules are inherited by all Monitoring Checks; however, you can configure maintenance schedules for each check individually in the **Advanced tab** of the **Monitoring Check properties**. Let's say a company has maintenance on every Friday at 11:00 pm for nearly all servers (use the global maintenance schedules for that). But for one server (server 'A'), maintenance is scheduled on Saturday at 09:00 am. Configure individual maintenance schedules for server 'A'.

3.16. Dependencies

Dependencies allow you to create a hierarchy of checks that depend on each other. This hierarchy is not related to the Folder structure of your Network Monitor configuration. Dependencies prevent you and your network administrators from being overwhelmed with notifications when a central router or server goes down. Without a dependency configuration, the failure of a central server or device would cause a failure of other servers, and as a result many notifications would be sent out. There are at least two items involved when configuring dependencies:

- ◆ **Dependee** - the computer/device that plays a central role. A failure of this 'Dependee' device or server would cause failures of other servers and devices (so called 'Dependers');
- ◆ **Depender(s)** - servers, devices or folders that depend on the 'Dependee'.

A dependee cannot be a folder, only a check. You can make other checks and/or folders dependent on the Dependee. It is recommended to use Folders rather than Checks as a Depender, because it is dynamic.

For more information about Dependencies, visit the [Online Dependency Guidelines](#) on the ActiveXperts web site. It contains a good sample and some best practice hints.

3.17. Backup and Restore

The ActiveXperts Network Monitor configuration is stored in one single file: `CONFIG.MDB`. The `CONFIG.MDB` is located in the `<Installation-Directory>\Configuration` directory.

Custom scripts are stored in the <Installation-Directory>\Scripts directory.

It is recommended to backup the configuration and custom scripts regularly.


▼ Manual Backup

To backup the configuration manually, follow the instructions as described in Chapter 3.3 ('Import, Export and Clear configuration settings') of this manual. This chapter also describes how to restore the configuration manually.

▼ Automatic Backup


Automatic Backup is enabled by default, and will backup the configuration file and all VBScript programs to a fixed network location automatically. By default, the backup is made on every Wednesday and Saturday, at 06:00am.

To change the Auto Backup settings:

- ◆ Select **Options** from the **Tools menu**, or press  on the toolbar.
- ◆ Select the **Auto Backup tab**;
- ◆ You can now **Enable/Disable** Auto Backup. When enabling Auto Backup, you must select at least one **Day of the Week** to schedule your backup. Choose a valid **Destination Directory** to backup your files to. It is recommended to choose a Network Location that is part of your daily overall backup procedure.

4. Managing Monitoring Checks


4.1. Adding a New Check

To quickly add a new Monitoring Check, click New Monitor Check  on the toolbar.

To add a new Monitoring Check:


- ◆ On the **Monitor menu**, click **New Monitoring Check**;
- ◆ In the **Check What** drop-down box, select the type of check. In the next chapter, Monitoring Checks are described in more detail;
- ◆ In the **Display Name** box, edit a custom display name; this name will also be used in the log files and reports;
- ◆ In the **Check every** field, specify how often a check should run. By default, a check will be monitored once every 30 seconds. This default can be changed from the **Options dialog** in the **Tools Menu**. To use a scheduled check instead of running it at specific intervals, use the 'Schedule this Check' option (see below) instead of the 'Check every' option;
- ◆ In the **Check fails after** field, specify the number of consecutive errors that must occur before a check will be considered as Failed; by default, a check will be considered as Failed after 3 consecutive errors;
- ◆ In the **Schedule this Check** fields, you can define at what times the check should run.

4.2. Copy/Paste a Check

To quickly copy an existing Monitoring Check to the Clipboard, click **Copy**  on the toolbar.

To copy an existing Monitoring Check:

- ◆ On the **Edit menu**, click **Copy**;


To quickly paste a Monitoring Check from the Clipboard, click **Paste**  on the toolbar.

To paste a Monitoring Check:

- ◆ On the **Edit menu**, click **Paste**;

Note: You can only copy **one** Monitoring Check to the clipboard at a time.

4.3. Deleting a Check

To quickly delete an existing Monitoring Check, click **Delete**  on the toolbar.

To delete an existing Monitoring Check:

- ◆ On the **Monitor menu**, click **Delete**;
- ◆ Confirm that you really want to remove the server from the configuration.

4.4. Editing a Check

To quickly edit the Monitoring Check properties, right click on the Monitoring Check and choose properties, or double click on the Monitoring Check.

The Monitoring Check dialog will pop up. This dialog contains 4 tabs:

- ◆ **General Properties;**
- ◆ **Notifications** – E-mail, SMS, Pager, SNMP Trap and Network/NetBIOS notifications;
- ◆ **Actions** – Run batch file, exe-file or VBScript programs; restart service(s) or reboot server;
- ◆ **Advanced Properties** – Configure Notification Frequency (re-notifications), Action Frequency (re-run programs), Maintenance hours and Dependencies.

▼ General Properties

Select the **General Properties tab**, and configure the following fields:

- ◆ **Check What** – select the type of check, for instance: ICMP;
- ◆ In the **Display Name** box, edit a custom display name; this name will also be used in the log files and reports;
- ◆ In the **Check every** field, specify how often a check should run. By default, a check will be monitored once every 30 seconds. This default can be changed from the **Options dialog** in the **Tools Menu**. To use a scheduled check instead of running it at specific intervals, use the 'Schedule this Check' option (see below) instead of the 'Check every' option;
- ◆ In the **Schedule this Check** fields, you can define at what times the check should run;
- ◆ In the **Check fails after** field, specify the number of consecutive errors that must occur before a check will be considered as Failed; by default, a check will be considered as Failed after 3 consecutive errors.

▼ Notifications Properties

Select the **Notifications tab**, and configure the following fields:

- ◆ **E-mail: Notify when check fails** – If the check fails, send an e-mail notification to the selected recipients. The recipients are either defined in the global Address Book, or configured for this particular check only;
- ◆ **E-mail: Notify when check recovers from a failed state** – If the check changes from Failure to Success, send an e-mail notification to the selected recipients;
- ◆ **Network: Notify when check fails** – If the check fails, send a network notification to the selected recipients;
- ◆ **Network: Notify when check recovers from a failed state** – If computer /device turns from offline to online, send a network notification to the selected recipients;
- ◆ **SMS/Pager: Notify when check fails** – If the check fails, send an SMS notification to the selected recipients;
- ◆ **SMS/Pager: Notify when check recovers from a failed state** – If computer /device turns from offline to online, send an SMS notification to the selected recipients;
- ◆ **SNMP Trap: Notify when check fails** – If the check fails, send an SNMP Trap notification to the selected recipients;
- ◆ **SNMP Trap: Notify when check recovers from a failed state** – If computer /device turns from offline to online, send an SNMP Trap notification to an SNMP network management system.

For all of the above items (except SNMP Traps), you can select recipient groups from the global Address Book.

If you want to use different recipients (or traps) for a particular Monitoring Check, press the '...' **button** next to the corresponding item.

▼ Actions

You can define an action for each particular check. Actions are triggered when a check fails, or when a check recovers from a failure. There are no general settings for Actions; all settings are made in the properties of the monitoring check.

There are 3 different types of actions:

- ◆ Restart service
After a failure, it's possible to restart a service. For instance, if you can't reach an IIS web server in your LAN, it may be a good idea to restart the W3SVC service. You can use either the short service name (for instance W3SVC) or the long service name (for instance: World Wide Web Publishing Service). To restart multiple services, enter all services separated by a semicolon (;), for instance: alerter;browser;
- ◆ Reboot computer
In some situations, it may be useful to reboot a machine to try to recover from a failure;
- ◆ Run Program
You can configure to run a program after a failure has occurred. ActiveXperts Network Monitor supports three different types of programs:
 - Executable files;
 - Batch programs;
 - VBScript programs.You can pass parameters to these programs on the command line. You can also use Notification Variables as parameters, as described in Appendix C.

To configure Actions, select the **Actions tab**, and configure the following fields:

- ◆ **Run this program (.exe or .bat) when check fails** – If server/device goes offline, run the specified Win32 executable or batch file on the ActiveXperts Network Monitor server;
- ◆ **Run this program (.exe or .bat) when check recovers from a failed state** – If server/device turns from offline to online, run the specified Win32 executable or batch file on the ActiveXperts Network Monitor server;
- ◆ **Run this program (.vbs) when check fails** – If server/device goes offline, run the specified Visual Basic script on the ActiveXperts Network Monitor server;
- ◆ **Run this program (.vbs) when check recovers from a failed state** – If server turns from offline to online, run the specified Visual Basic script on the ActiveXperts Network Monitor server.
- ◆ **No reboot/restart after failure** – No reboot or restart of a service when failure occurs;
- ◆ **After failure, reboot computer** – Upon failure, reboot a particular server;
- ◆ **After failure, restart service(s)** – Upon failure, restart a service on a particular server. You can restart multiple services by providing a list of services. A list of services should contain individual services, separated by the ';' character.

To restart a service or reboot a computer, the Network Monitor service credentials are used by default (i.e. the credentials used to start the ActiveXperts Network Monitor service, see also the "Services" applet in the "Administrative Tools" folder). However, if a server is in a different domain or forest, and there is no trust, you may need to pass different credentials to restart or reboot. To do so, press the **Credentials button** and select an entry from the **Alternate Credentials list**. Alternate credentials are administrated globally (see also chapter 3.7: "Options")

▼ Advanced

Select the **Advanced tab** to configure the following items:

- ◆ **Notification Frequency** – This only applies to Failed checks. By default, notifications are sent only once after failure; if you prefer repetitive notifications, select the **Notify every** radio button and enter the notification frequency;
- ◆ **Action Frequency** – This only applies to Failed checks. By default, actions are invoked only once after failure; if you prefer repetitive actions, select the **Trigger every** radio button and enter the frequency;
- ◆ **Server Maintenance periods** – If you need Maintenance Schedules for a particular check other than the global Maintenance Schedules, you can configure it here.
- ◆ **Dependencies** – Read-only view of the dependencies for this check;
- ◆ **Check ID** – Each check has a unique ID. This ID is the key in the [Nodes] table of the configuration database (CONFIG.MDB).

4.5. Monitoring servers in the same domain

The ActiveXperts Network Monitor engine runs as a service on a Windows 2008/Vista/2003/2000/XP operating system. This service runs with Local System credentials or with Local/Domain Administrator credentials.

To change the ActiveXperts Network Monitor service credentials:

- ◆ Open the **Computer Management** application that is part of the Operating System;
- ◆ Click on the **Services applet**;
- ◆ Select the **ActiveXperts Network Monitor service** and click on the **Log On tab**;
- ◆ Choose **This Account** and enter the Account and Password information.

To monitor servers in a domain, enter an account that has Administration privileges on all domain members. A 'Domain Administrator' or 'Enterprise Administrator' account will suffice. You can use the UNC notation for the domain account, i.e.: DOMAIN\Account. You can also use other dotted domain notations (mysubdomain.mydomain.dom\Account) or user principle names (j.doe@mydomain.dom).

4.6. Monitoring servers in the other domains

To monitor servers in another domain, ActiveXperts Network Monitor requires administrator rights on that domain. This can be established through a trust relationship between these domains. However, if there is no trust relationship, the service account credentials cannot be used.

To monitor servers in another – untrusted – domain, you need to enter credentials for each Windows server in the **Server Credentials** table. See also Chapter 3.7: "Options". This also applies to stand-alone servers.

4.7. Configuring a Check

When you add a new Monitoring Check, you must select the type of Check. ActiveXperts Network Monitor supports a wide range of built-in checks. This paragraph describes how to configure each built-in check.

4.7.1 IP-related checks

▼ DNS Server check

ActiveXperts Network Monitor can resolve any DNS record and check the result against a specified value. Allowed record types include the 'A' record, 'MX' record' and 'CNAME' record'.

A DNS Server check requires the following parameters:

- ◆ **DNS Server** – The IP address or hostname of the DNS server that you want to check;
- ◆ **Name** – The DNS name to resolve;
- ◆ **Type** – The DNS record type of the DNS record. Valid record type are: 'A Record', 'MX Record' 'CNAME Record' or 'Any Record';
- ◆ **IP address(es)** – The expected IP number(s). If the query result does not include the given IP address, the check will fail. Otherwise, the check will succeed. Please note that a DNS query can return more than one IP address.
In case the 'Type' was set to 'CNAME Record', the expected result is a host name, not an IP address.

▼ FTP check

ActiveXperts Network Monitor can check the availability of an FTP site.

You must pass credentials (username and password) to access the actual FTP site. If the FTP server allows anonymous access, specify 'anonymous' in the 'Account' field, and specify a valid e-mail address in the 'Password' field.

With the FTP check, you can check for a file in one of the subdirectories on the FTP server, and even check for a specific pattern in the file.

An FTP check requires the following parameters:

- ◆ **Host** – Hostname or IP address of the remote FTP server. If the remote FTP server is listing on a port other than 21, you can append it to the host, like this: 192.168.0.1:23
- ◆ **Passive** – Specifies the way ActiveXperts Network Monitor establishes a connection with the FTP server: in Passive mode or in Active mode. Default: Passive.
- ◆ **FTP Account** – Account used to access the FTP server. You cannot leave it blank. If the FTP server allows anonymous access, you must specify 'anonymous' in the 'Account field' and a valid e-mail address in the 'Password' field;
- ◆ **FTP Password** – Password used to access the FTP server. If the FTP server allows anonymous access, you must specify 'anonymous' in the 'Account field' and a valid e-mail address in the 'Password' field;
- ◆ **Anonymous** – If the FTP server allows anonymous access, you can click on this check box to enter credentials automatically in the 'Account' and 'Password' fields. The 'Anonymous' property is not used by the engine;
- ◆ **Check Connectivity only / Check File Existence** – If you want to check availability only, you should select 'Check Connectivity' here. If you want to check for existence of a particular file, you must select 'Check File Existence';
- ◆ **Directory** – If you check for file existence, you can specify a working directory where the file indicated by the 'File' field should be located. Leave it blank to use the root of the FTP site as the working directory;
- ◆ **File** – The file you want to check;
- ◆ **Check file existence only / Check for a specific pattern in the file** – You can check for file existence only, or for a specific pattern in the file;
- ◆ **Use binary file transfer** – Indicates how the file should be transferred so it can be analyzed. Only possible if 'Check for a specific pattern in the file' is selected;

- ◆ **Pattern should (not) match** – If the pattern is matched, then the result of the check can be either success or error.

▼ SFTP check

ActiveXperts Network Monitor can check the availability of an SFTP server.

SFTP (Secure File Transfer Protocol) allows secure network file transfer over an insecure network, such as the Internet. The Secure File Transfer Protocol is an extension to the SSH version 2.0 protocol. Most SSH server implementations will also allow for SFTP logins. SFTP is the secure successor to FTP.

An SFTP check requires the following parameters:

- ◆ **SFTP Host** – Hostname or IP address of the remote SFTP server;
- ◆ **Port** – Port of the SFTP daemon on the remote SFTP host. Default: port 22;
- ◆ **Account** – Account used to access the SFTP server;
- ◆ **Password** – Password to authenticate to the SFTP server. If omitted, you must set a valid Private Key File;
- ◆ **Private Key File** – Private Key File to authenticate to the SFTP server. If omitted, you must set a valid Password;
- ◆ **Accept Host Key** – Specifies whether to accept an unknown or changed host key;
- ◆ **Check Connectivity only / Check File Existence** – If you want to check availability only, you should select 'Check Connectivity' here. If you want to check for existence of a particular file, you must select 'Check File Existence';
- ◆ **File (Full Path)** – The file you want to check;
- ◆ **Check file existence only / Check for a specific pattern in the file** – You can check for file existence only, or for a specific pattern in the file;
- ◆ **Pattern should (not) match** – If the pattern is matched, then the result of the check can be either success or error.

▼ TFTP check

ActiveXperts Network Monitor can check the availability of a TFTP host by checking the existence of a file on the TFTP host. TFTP stands for 'Trivial File Transfer Protocol' and is a forerunner of the FTP protocol. It has less functionality than FTP: it is based on the (unreliable) UDP protocol, has no support for directory browsing and has not protected by a logon and password.

With the TFTP check, you can check for a file in a directory on the TFTP host, and check for a specific pattern in the file.

A TFTP check requires the following parameters:

- ◆ **Host** – Hostname or IP address of the remote TFTP server. If the remote TFTP server is listening on a port other than 69, you can append it to the host, like this: 192.168.0.1:8069
- ◆ **File** – The file you want to check;
- ◆ **Check file existence only / Check for a specific pattern in the file** – You can check for file existence only, or for a specific pattern in the file;
- ◆ **Use binary file transfer** – Indicates how the file should be transferred so it can be analyzed. Only possible if 'Check for a specific pattern in the file' is selected;
- ◆ **Pattern should match / Pattern should not match** – If the pattern is matched, then the result of the check can be either success or error.

▼ HTTP/HTTPs check

ActiveXperts Network Monitor can check the availability of HTTP and HTTPs sites, on default ports (i.e.: 80 and 443) or on alternate ports.

If the HTTP(s) server is not directly accessible, you can configure ActiveXperts Network Monitor to go through a Proxy server to access the particular HTTP(s) server, even passing credentials for that Proxy server (to be able to make use of the Proxy).

Additionally, you can pass credentials (username and password) to access the actual HTTP(s) site if required. ActiveXperts Network Monitor supports web site content checking; contents of web sites can be searched for text patterns (including tags).

An HTTP/HTTPs check requires the following parameters:

- ◆ **URL** – The location of the website in URL format (i.e. `http://server[:port]/path/...` format);
- ◆ **Require Server verification** – A flag to indicate: HTTP or HTTPs;
- ◆ **Check for availability only / Page must contain pattern / Page must not contain pattern** – In case of 'Check for Availability only', only the availability of the site is checked. In case of 'Page must (not) contain string', the content of the URL is checked for specific contents;
- ◆ **Time-out after** – Time-out in seconds. If the time-out expires, the result is 'Error';
- ◆ **Use website authentication** – A flag to indicate whether authentication is required for the web site or not. If authentication is required, 'Website Account' and 'Website Password' must be provided;
- ◆ **Website Account** – A valid account on the web site;
- ◆ **Website Password** – A valid password for the account on the web site;
- ◆ **Use a Proxy server** – A flag indicating whether the web site should be accessed through a Proxy server or not;
- ◆ **Proxy** – If the 'Use a Proxy server' field is set, this field indicates the actual Proxy server. A hostname, NetBIOS name or IP address is required here;
- ◆ **Proxy authentication** – If the 'Use a Proxy server' flag is set, and the proxy server indicated by the 'Proxy' field requires authentication, enable this check box;
- ◆ **Proxy Account** – A valid account on the Proxy server;
- ◆ **Proxy Password** – A valid password for the account on the Proxy server.

▼ ICMP/Ping check

ICMP Ping checks a remote host for availability. Local hosts should normally respond to ping requests within milliseconds. However, on a very congested network it may take up to 3 seconds or longer to receive an echo packet from the remote host.

If the time-out is set too low under these conditions, it will appear that the remote host is not reachable (which is almost the truth).

ActiveXperts Network Monitor checks servers for availability by sending ICMP Echo commands and wait for the responds. An ICMP time-out failure doesn't necessarily mean that the remote host is actually functioning beyond its ability to echo packets.

An ICMP/Ping check requires the following parameters:

- ◆ **Host** – The DNS name or IP address of the computer you want to ping (can even be a WINS name, but only if the name can be resolved by some WINS server in the network);
- ◆ **Time-out after** – Maximum number of milliseconds it should take before a response is received;
- ◆ **Number of retries** – The number of retries to send when a ping fails;
- ◆ **Time to Live** – Maximum Time to Live (TTL) value;
- ◆ **Buffer Size (bytes)** – Send buffer size.

▼ IMAP Mail Server availability check

ActiveXperts Network Monitor can check IMAP mail servers by establishing a connection on the remote IMAP port (usually port 143) and do a handshake. By handshaking, ActiveXperts Network Monitor can verify that the remote server's IMAP protocol is working well.

An IMAP Mail Server check requires the following parameters:

- ◆ **Host** – Hostname or IP address of the server to be monitored;
- ◆ **Port** – TCP port number of the IMAP protocol. Default: 143;
- ◆ **Send command when connected** – As soon as connection is established, send a command. By default, no command string will be sent;
- ◆ **Response must include string** – when connected, optionally send a command. Then wait for the response. The default response for IMAP servers includes: 'IMAP';
- ◆ **Time-out** – Number of milliseconds before the check will time-out. Usually, a connection to the server will be established within 1 second. However, some slow/busy servers need more time. Recommended value is 7000 milliseconds.

▼ LDAP check

LDAP (Lightweight Directory Access Protocol) is a protocol for querying (and modifying) directory services like Microsoft Active Directory and Novell Netware.

The LDAP check requires just one parameter:

- ◆ **LDAP Server** – Hostname or IP address of the server to monitor.

The check will by default try to retrieve the full name of the queried directory service, and match the result against a pattern. One may check want to use more sophisticated queries; for this reason, the check is a VBScript check to allow customization.

▼ NNTP News Server check

ActiveXperts Network Monitor can check NNTP news servers by establishing a connection on the remote TCP port (usually port 119) and do a handshake. By handshaking, ActiveXperts Network Monitor can verify that the remote server's NNTP protocol is working well.

An NNTP News Server Availability check requires the following parameters:

- ◆ **Host** – Hostname or IP address of the server to be monitored;
- ◆ **Port** – TCP port number of the NNTP protocol. Default: 119;
- ◆ **Send command when connected** – As soon as connection is established, send a command. By default, no command string will be sent;
- ◆ **Response must include string** – When connected, optionally send a command. Then wait for a response. The default response for NNTP servers includes: '200';
- ◆ **Time-out** – Number of milliseconds before the check will time-out. Usually, a connection to the server will be established within 1 second. However, some slow/busy servers need more time. Recommended value is 7000 milliseconds.

▼ NTP Time Server check

Commercial organizations today rely on networks of computers, all of which have clocks that are the source of time for files or operations they handle.

Most of these organizations use a time server to ensure accurate time settings. The NTP protocol is the protocol used to synchronize times between workstations and servers, and external time

sources. ActiveXperts Network Monitor uses the IP based NTP protocol to check availability of internal and external time sources.

An NTP check requires one parameter:

- ◆ **Time Server** – Hostname or IP address of the time server.

▼ POP3 Mail Server check

ActiveXperts Network Monitor can check POP3 mail servers by establishing a connection on the remote TCP port (usually port 110) and do a handshake. By handshaking, ActiveXperts Network Monitor can verify that the remote server's POP3 protocol is working well.

A POP3 Mail Server Availability check requires the following parameters:

- ◆ **Host** – Hostname or IP address of the server to be monitored;
- ◆ **Port** – TCP port number of the POP3 protocol. Default: 110;
- ◆ **Send command when connected** – As soon as connection is established, send a command. By default, no command string will be sent;
- ◆ **Response must include string** – When connected, optionally send a command. Then wait for a response. The default response for POP3 servers is: '+OK POP3';
- ◆ **Time-out** – Number of milliseconds before the check will time-out. Usually, a connection to the server will be established within 1 second. However, some slow/busy servers need more time. Recommended value is 7000 milliseconds.

▼ RADIUS check

ActiveXperts Network Monitor can check RADIUS (Remote Authentication Dial In User Service) servers by authenticate a user.

A RADIUS check requires the following parameters:

- ◆ **RADIUS Server** – Hostname or IP address of the server to be monitored;
- ◆ **RADIUS UDP Port** – UDP port number of the RADIUS protocol. Default: 1812;
- ◆ **Timeout** – Number of milliseconds before the check will time-out;
- ◆ **User** – User to authenticate against the RADIUS server;
- ◆ **Password** – Password of the user;
- ◆ **Secret** – RADIUS secret.

▼ SMTP Mail Server check

ActiveXperts Network Monitor can check SMTP mail servers by establishing a connection on the remote TCP port (usually port 25) and do a handshake. By handshaking, ActiveXperts Network Monitor can verify that the remote server's SMTP protocol is working well.

An SMTP Mail Server check requires the following parameters:

- ◆ **Host** – Hostname or IP address of the server to be monitored;
- ◆ **Port** – TCP port number of the SMTP protocol. Default: 25;
- ◆ **Send command when connected** – As soon as connection is established, send a command. By default, no command string will be sent;
- ◆ **Response must include string** – when connected, optionally send a command. Then wait for the response. The default response for SMTP servers includes: '200';
- ◆ **Time-out** – Number of milliseconds before the check will time-out. Usually, a connection to the server will be established within 1 second. However, some slow/busy servers need more time. Recommended value is 7000 milliseconds.

▼ SMTP to POP3 check

This check verifies whether an e-mail service is working properly by sending a test e-mail message through an SMTP server and verifying that it has been delivered to the recipient's mailbox.

An SMTP to POP3 check requires the following parameters:

- ◆ **E-mail Recipient** – E-mail address of the recipient to send the e-mail to;
- ◆ **Subject** – Subject of the e-mail. Note that the ActiveXperts engine will add a unique ID to it, to mark the e-mail as an SMTP to POP3 test mail;
- ◆ **SMTP Server** – select what SMTP server to use: the global primary SMTP server, the global secondary server, or another SMTP server;
- ◆ **POP3 Server** – the hostname or IP address of the POP3 server;
- ◆ **POP3 Account** – the account to authenticate to the POP3 server;
- ◆ **POP3 Password** – the password to authenticate to the POP3 server;
- ◆ **Check E-mail every** – check interval, in minutes;
- ◆ **Check fails if e-mail is not received within** – e-mail delivery time-out value. If the e-mail is not delivered to the POP3 box within the specified time, the check will fail;
- ◆ **Delete the mail after delivery** – Network Monitor can optionally delete the e-mail once it has been delivered.

▼ SNMP GET check

SNMP means: Simple Network Management Protocol. The SNMP GET message allows the Network Monitor Engine to request information about a specific variable on a remote computer or device. The agent, upon receiving a GET message, will issue a GET-RESPONSE message to the Network Monitor Engine with either the information requested or an error indication as to why the request cannot be processed.

An SNMP GET check requires the following parameters:

- ◆ **Host** – Hostname or IP address of the computer/device to monitor;
- ◆ **Port** – UDP port used for SNMP on the target machine/device. Default port is 161;
- ◆ **Community** – The SNMP community string; Default: 'public';
- ◆ **Protocol** – Indicates how the SNMP client should communicate with the remote SNMP agent. If you choose 'Automatic', the SNMP agents on both sites will negotiate and use the preferred protocol. Choose 'SNMPv1' to force the agents to use SNMP version 1; choose 'SNMP v2c' to force the agents to use SNMP version 2c;
- ◆ **OID (Numeric/Symbolic)** – The Object ID; the OID is a long numeric tag or a symbolic (friendly) name, used to distinguish each variable uniquely in the MIB and in SNMP messages. If you use the numeric tag format, the OID can be prefixed by a '.'. This is optional. For example: .1.3.6.1.2.1.1.5.0 or 1.3.6.1.2.1.1.5.0. Friendly names are names like: system.sysName.0, or interfaces.ifTable.ifEntry.ifOperStatus.1.
- ◆ **Select a symbolic OID from a MIB file...** – Use this button to select an alpha-numeric OID from a MIB file. You can use virtually any 3rd-party MIB file;
- ◆ **OID Data Type** – The OID Data type. The following type are valid data types: Bit Stream, Counter, Integer, IP address, Object Identifier, Opaque String, String, Time Ticks and Unsigned Integer;
- ◆ **OID Data must be** – Choose the condition: Equal To, Not Equal To, Less Than, Less or Equal To, Greater Than, Greater or Equal To. This condition is used to compare the actual SNMP value against the 'IOD Data Value';
- ◆ **OID Data Value** – OID value that will be compared against the actual OID value, using the 'OID Data must be' operand;

- ♦ **AND / OR** – To extend the condition, use AND or OR operator. On selecting AND or OR, you must specify an additional condition (Equal To, etc.) and OID Data Value.

▼ SNMP Trap Receive check

The SNMP Trap Receive check listens for real-time network traps for processing. The SNMP Trap Receiver must be enabled at a global level. To enable the SNMP Trap Receiver:

- ♦ On the **Tools menu**, choose **Options**;
- ♦ Select the **Advanced Tab** and click on the **Configure SNMP Trap Receiver button**;
- ♦ Enable the Trap Receiver by enabling the **Enable SNMP Trap Receiver** checkbox.

An SNMP Trap Receive check works different than other checks in Network Monitor: the SNMP Trap Receive check is event-driven. The check is not executed at timed intervals, but is triggered on a newly received trap. As a result, you cannot specify a time interval for SNMP Trap Receive checks.

An SNMP Trap Receive check requires the following parameters:

- ♦ **Receive from Host** – Hostname or IP address of the computer/device to monitor. To specify any host, use '*';
- ♦ **Receive OID** – The Object ID to receive. This can be a numeric OID or a symbolic OID. Type '*' to check for any OID;
- ♦ **Select a symbolic OID from a MIB file...** – Use this button to select an alpha-numeric OID from a MIB file. You can use virtually any 3rd-party MIB file;
- ♦ **Receive OID Data Type** – The expected OID Data type. The following type are valid data types: Bit Stream, Counter, Integer, IP address, Object Identifier, Opaque String, String, Time Ticks and Unsigned Integer;
- ♦ **Match OID Value** – To check the OID data for specific value(s), enable this check box and configure the conditions in the same way as for the 'SNMP GET' check.

▼ TCP/IP check

ActiveXperts Network Monitor can check local- or remote servers by challenging a specific port. It makes a connection to it, and performs a challenge/respond (by sending a sequence of bytes to it, wait for the respond and analyzing the received information).

A TCP/IP check requires the following parameters:

- ♦ **Host** – Hostname or IP address of the server to be monitored;
- ♦ **Port** – TCP port number of the protocol to be checked;
- ♦ **Send command when connected** – As soon as connection is established, send a command;
- ♦ **Response must include string** – When connected, optionally send a command. Then wait for a response;
- ♦ **Time-out** – Number of milliseconds before the check will time-out. Usually, a connection to the server will be established within 1 second. However, some slow/busy servers need more time. Recommended value is 7000 milliseconds.

4.7.2 Microsoft Windows-related checks

▼ Active Directory check

The Active Directory check monitors services, processes and WMI counters related to Microsoft Active Directory.

The Active Directory check requires the following parameters:

- ◆ **Services** – A list of Active Directory services that should be running on the target computer;
- ◆ **Processes** – A list of Active Directory processes that should be running on the target computer. For each process, you can specify a maximum CPU usage and a maximum memory usage;
- ◆ **WMI Performance Counters** – A list of Active Directory performance counters that should be monitored.

▼ Anti-Virus/Anti-Spam check

The Anti-Virus check allows monitoring various popular Anti-Virus packages on workstations and servers. The following Anti-Virus software packages are supported:

- ◆ Avast;
- ◆ AVG;
- ◆ Avira;
- ◆ BitDefender;
- ◆ BullGuard;
- ◆ Eset NOD32;
- ◆ F-Secure;
- ◆ G Data;
- ◆ Kaspersky;
- ◆ McAfee;
- ◆ Norman;
- ◆ Norton;
- ◆ Panda;
- ◆ Sophos;
- ◆ Trend Micro.

An Anti-Virus/Anti-Spam check requires the following parameters:

- ◆ **Services** – A list of services that should be running on the target computer;
- ◆ **Processes** – A list of processes that should be running on the target computer. For each process, you can specify a maximum CPU usage and a maximum memory usage;
- ◆ **WMI Performance Counters** – A list of performance counters that should be monitored.

▼ CPU Usage check

ActiveXperts Network Monitor provides the 'CPU Usage' check to monitor processor(s) on Windows platforms. When the CPU load exceeds the limit, an alert is generated.

For multi-processor systems, you can select to monitor all CPU's (default) or monitor an individual CPU.

A CPU Usage check requires the following parameters:

- ◆ **Computer** – The NetBIOS name, DNS name or the IP address of the computer you want to monitor;

- ♦ **CPU** – Select 'All CPU's' or 'This CPU'; on a multi-processor system, you can monitor a specific CPU ('This CPU'). To monitor all processors on a single- or multi-processor system, select 'All CPU's';
- ♦ **Max. CPU Usage** – Maximum allowed CPU usage (%).
- ♦ **Credentials** – Select alternate Windows credentials if necessary.

▼ Directory check

You are running Windows Server and some of your users insist on copying the contents of their notebook computer to your file server. Other users want to download everything they see on the Web. Unfortunately, you're running out of disk space. Disk space is your server's most expensive subsystem, so it's a good practice to monitor – for instance - user's Home Directories. The 'Directory check' can be of good help.

A Directory check requires the following parameters:

- ♦ **Directory** – The directory in UNC ('Universal Naming Convention') format. For instance: `\\server01\public\docs`;
- ♦ **Check Directory Existence Only / Check Directory Size / Check File Count / Check Directory Content Change** – Select the type of Directory check;
- ♦ **Minimum/Maximum size** – Minimum or maximum size (MB) of the directory (only applicable if 'Check Directory Size' is selected);
- ♦ **Minimum/Maximum number** – Minimum or maximum of files in a directory (only applicable if 'Check File Count' is selected). If you want to count a directory as a file, select '**Also count a directory as a file**';
- ♦ **Include subdirectories** – select this option to include subdirectories in any type of directory check;
- ♦ **Credentials** – Select alternate Windows credentials if necessary.

▼ Disk Drives check

ActiveXperts Network Monitor can monitor all physical disk drives on servers running the Windows operating system. If a malfunctioning disk drive is detected on the computer, an alert is generated.

A Disk Drive check requires the following parameters:

- ♦ **Computer** – The host name or the IP address of the computer you want to monitor;
- ♦ **Credentials** – Select alternate Windows credentials if necessary.

▼ Disk Space check

The amount of free disk space is checked periodically, and if it drops too low you're immediately notified. It can also notify if used space gets too high.

A Disk Space check requires the following parameters:

- ♦ **Computer** – The host name or the IP address of the computer you want to monitor;
- ♦ **Drive** – the drive letter as it appears on the remote server;
- ♦ **Disk Space – Maximum allowed space / Minimum required free space** – In case of 'Minimum required free space', the computer is checked for a minimum available space specified by the number of MB's that you enter. In case of 'Maximum allowed used space', the computer is checked for a maximum used space specified by the number of MB's that you enter;
- ♦ **MB / GB / %** – the upper/lower limit in Megabytes, Gigabytes or percentage;

- ◆ **Credentials** – Select alternate Windows credentials if necessary.

Note: The 'Disk Space' check uses the system's administrative shares (i.e. C\$, D\$ etc.) to access drives on remote computers. For security reasons, these share are sometimes renamed by system administrators, for instance: **MYCDRIVE\$**. You can type such a name in the selection box, and the Network Monitor Engine will use this administrative share name instead of the defaults administrative share name.

▼ Event Log check

ActiveXperts Network Monitor can read Windows Event logs on local- or remote computers. It can look for specific Event Sources, Categories, Event ID's and so on. It can look for a pattern in the Description of the Event.

It can do advanced filtering in Event Logs; it can look for multiple events in the Event Log, and notify the system administrator if one of the Events occurred in a specific time interval. For instance, as a network administrator, you want an alert if there's a McAfee or Norton virus message in the Application Event Log, but only if the event is posted in the last 30 minutes. ActiveXperts Network Monitor uses VBScript and WMI for this.

It enables you to fully customize Event Log filtering, speeding up performance by checking for more than one event in each cycle.

An Event Log check requires the following parameters:

- ◆ **Computer** – The host name or the IP address of the computer you want to monitor;
- ◆ **Log File** – The Log File to be checked. Choose the appropriate log file, for instance: 'Application', 'Security', 'System', or server-related log (like DNS, Exchange, etc.);
- ◆ **Credentials** – Select alternate Windows credentials if required;
- ◆ **Information/Warning/...** – Filter these event types;
- ◆ **Source** – Filter events that match this Event Source;
- ◆ **Category** – Filter events that match this Event Category;
- ◆ **ID** – Filter events that match this Event ID;
- ◆ **User** – Filter events that match this User;
- ◆ **Description matches string** – Filter events that match the description string in the Event Message;
- ◆ **Only Events from the last x minutes** – This options allows you to discard errors that happened in the past. For instance, if you don't want to be notified about error events that happened in the past (like a week ago), use this option;
- ◆ **This check will fail if such event is found/not found** – Specify whether this check will fail or succeed when an event is found.

▼ File check

ActiveXperts Network Monitor can monitor file existence, file size and file content. This is particularly useful in situation where log files need to be analyzed. In many organizations, batch jobs run at night and produce logging information; ActiveXperts Network Monitor can check this logging information and analyze it. It can check the existence, or search for patterns. It can also check the size of a file.

A File check requires the following parameters:

- ◆ **File (UNC Path)** – The path of the file to be checked in UNC format (i.e. \\server\share\... syntax);
- ◆ **Check for: Existence only / Maximum Size / Pattern** – Choose an option: just checks the existence, or check the size of a file (in KB/MB), or search for a pattern in the file

- ◆ **If condition should be True/False** – If the file conditions are true, then the result of the check is: success; otherwise, the result will be: error;
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

▼ Memory Usage check

ActiveXperts Network Monitor can check the memory usage of the Windows Operating System. It can monitor the total available physical memory usage, the committed memory or the pages per second.

A Memory Usage check requires the following parameters:

- ◆ **Computer** – Host name or IP address of the computer to monitored;
- ◆ **Memory** – select 'Minimum required Available Physical Memory' to check physical available memory; choose 'Maximum allowed Committed Memory' to check committed memory; choose 'Maximum allowed Pages Per Second' to check paging;
- ◆ **MB / Pages per Second** – enter the amount in MB's (for the physical memory and committed memory checks) or number of pages per second;
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

▼ MS Exchange Server check

ActiveXperts Network Monitor monitors the status of the Exchange services, and monitors the most important performance counters. Among these performance counters are: performance counters for the Information Store, mailboxes, public folders and SMTP connector. If it drops too low you're notified immediately.

One can extend the Exchange check function by checking more services and monitoring more performance counters.

The following MS Exchange versions are supported: 2007, 2003, 2000 and 5.x.

An MS Exchange Server check requires the following parameter:

- ◆ **Exchange Server** – The host name or IP address of the MS Exchange Server;
- ◆ **Exchange Server Version** – Version of Exchange Server. Can be either 2007, 2003, 2000 or 5.5;
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

▼ MS ISA Server check

ActiveXperts Network Monitor monitors the status of the MS ISA Server services. It can monitor a caching-only ISA server, a firewall-only ISA server, or an integrated (caching+firewall) ISA server. The following MS ISA Server versions are supported: 2006, 2004 and 2000.

An MS ISA Server check requires the following parameters:

- ◆ **ISA Server** – The host name or IP address of the ISA server;
- ◆ **ISA Server Version** – Version of ISA Server. Can be either 2006, 2004 or 2000;
- ◆ **ISA Server Mode** – Specifies in what mode the ISA Server is running: Caching Only, Firewall Only, or Integrated (Caching + Firewall);
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

▼ MS Message Queue (MSMQ) check

ActiveXperts Network Monitor monitors the status of the MS Message Queue's. It can check a queue for its length (i.e. number of jobs in the queue) or for its total size (MB).

An MSMQ check requires the following parameters:

- ◆ **Server** – The host name or IP address of the server;
- ◆ **Queue Name** – Name of the MSMQ queue, for instance: `private\admin_queue`;
- ◆ **Maximum Queue Length** – Maximum number of jobs allowed in the queue;
- ◆ **Maximum Queue Size** – Maximum amount of MB's in the queue;
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

▼ MS SharePoint Server check

ActiveXperts Network Monitor monitors the status of the MS SharePoint Server services. It can monitor the following MS SharePoint flavors: 'Microsoft Office SharePoint Portal Server 2007', 'Windows SharePoint Services 3.0 (framework for MOSS 2007)', 'Microsoft Office SharePoint Portal Server 2003' and 'Windows SharePoint Services 2.0 (framework for MOSS 2003)'.

An MS SharePoint Server check requires the following parameters:

- ◆ **SharePoint Server** – The host name or IP address of the SharePoint server;
- ◆ **SharePoint Version** – Version of SharePoint Server. Can be either 'Microsoft Office SharePoint Portal Server 2007', 'Windows SharePoint Services 3.0', 'Microsoft Office SharePoint Portal Server 2003' and 'Windows SharePoint Services 2.0';
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

▼ MS Terminal Server check

ActiveXperts Network Monitor monitors the status Terminal Server (part of Windows2008/Vista/2003/XP/2000) server by checking the number of active/inactive sessions.

A Terminal Server check requires the following parameters:

- ◆ **Terminal Server Computer** – The host name or IP address of the Terminal Server computer;
- ◆ **Maximum number of Active Sessions** – Maximum active sessions;
- ◆ **Maximum number of Inactive Sessions** – Maximum inactive sessions, i.e. disconnected and idle sessions;
- ◆ **Maximum number of Sessions** – Maximum number of active and inactive sessions;
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

▼ PowerShell check

PowerShell is a command line interface shell for Microsoft Windows platforms:

- ◆ It is a standard feature in Windows 7;
- ◆ It is included with Windows 2008 but not installed by default;
- ◆ It is available as a separate download for Windows 2003, Windows Vista and Windows XP;
- ◆ It is not available for Windows 2000 platforms;
- ◆ PowerShell is not available for Windows 2000 platforms.

ActiveXperts Network Monitor can check any Windows server by running a PowerShell script. The script is executed on the monitoring machine. There's no need to have PowerShell installed on the monitored server; it must be installed on the monitoring computer. PowerShell scripts do not need

to be copied to the monitored computer; you can have all PowerShell scripts located on the monitoring computer to monitor remote computers.

ActiveXperts Network Monitor ships with a collection of PowerShell (.ps1) that work out of the box.

ActiveXperts Network Monitor requires the PowerShell script output (i.e. StdOut) to be formatted according to the following syntax:

```
[SUCCESS | ERROR | UNCERTAIN]: { <explanation> } { DATA:<value>}
```

The <explanation> field is displayed in the 'Last Response' column in the Manager application. The <value> field is displayed in the 'Data' column in the Manager application.

Samples:

```
ERROR: Free Disk space is less than 40 GB DATA:34
SUCCESS: CPU Usage is 10%, maximum allowed is 50% DATA:10
```

A PowerShell check requires the following parameters:

- ◆ **Script File** – The PowerShell script. The script is executed on the monitoring computer;
- ◆ **Parameter1** – 1st parameter of the script (optional);
- ◆ **Parameter2** – 2nd parameter of the script (optional);
- ◆ **Parameter3** – 3rd parameter of the script (optional);
- ◆ **Parameter4** – 4th parameter of the script (optional);
- ◆ **Parameter5** – 5th parameter of the script (optional);
- ◆ **Parameter6** – 6th parameter of the script (optional);
- ◆ **If StdErr is not empty, the result will be** – If there's an error in the script, you can handle this error and specify what the result of the check should be: Uncertain, Error or Success;
- ◆ **Time-out** – Number of milliseconds before the check will time-out.

▼ Printer Availability check

Even the most mechanically sound printer stops working or needs maintenance from time to time: Printers run low on toner, run out of paper, or get jammed - unavoidable situations that prevent users from printing their documents. Unfortunately, when a printer stops working, no notice is sent to users; in addition, users can still send print jobs to the printer. If the problem is not identified and corrected, those jobs will continue to accumulate as long as the printer is unavailable. For these reasons, monitoring the printers in your organization is an important part of print management. With a well-designed monitoring strategy in place, you can receive timely notification whenever a printer stops functioning and take immediate steps to either get the printer back online or transfer print jobs to a different printer.

ActiveXperts Network Monitor checks printers for availability by checking its status. Windows knows a wide range of printer status values, like: 'Running', 'In Test', 'Power Off', 'Offline', 'Power Save', and so on.

If the Printer Status is not equal to Running or Power Save, then the printer is considered as malfunctioning.

A Printer Availability check requires the following parameters:

- ◆ **Print Server** – The hostname or IP address of the print server;
- ◆ **Printer Name** – The name of the printer, as it appears in the Windows' control panel. For instance: 'HP LaserJet 2300 Series PS';
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

Note: The printer availability check is based on WMI, and only works on Windows 2000 platforms or higher.

▼ Process

ActiveXperts Network Monitor allows users to check processes on local- and remote computers; if a process is active, a computer is considered available. Additionally, memory usage of a process can be checked, to detect memory leaks.

A Process check requires the following parameters:

- ◆ **Computer** – The host name or the IP address of the computer you want to monitor;
- ◆ **Process** – The module name of the process, including the extension. For instance: `alerter.exe`, or `explorer.exe`;
- ◆ **Check memory of this process** – Enable/disable memory checking of the particular process. Enter the maximum amount of memory (in MB) that a process may consume;
- ◆ **No process on this computer should consume more than** – Checks for any process using more than the specified amount of memory;
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

Note: The process check is based on WMI; it requires WMI on both monitored and monitoring system.

▼ Remote Command check

ActiveXperts Network Monitor can check any Windows server by executing a command on a remote computer. The command file (executable, batch-job, etc.) must be located on the remote monitored computer.

ActiveXperts Network Monitor requires the remote command output (i.e. StdOut) to be formatted according to the following syntax:

```
[SUCCESS | ERROR | UNCERTAIN]: { <explanation> } { DATA:<value>}
```

The `<explanation>` field is displayed in the 'Last Response' column in the Manager application. The `<value>` field is displayed in the 'Data' column in the Manager application.

Samples:

```
ERROR: Free Disk space is less than 40 GB DATA:34
SUCCESS: CPU Usage is 10%, maximum allowed is 50% DATA:10
```

A Remote Command check requires the following parameters:

- ◆ **Computer** – The host name or the IP address of the computer you want to monitor;
- ◆ **Command** – The command to execute on the remote computer. This command must reside on the remote computer;
- ◆ **If StdErr is not empty, the result will be** – If there's an error in the script, you can handle this error and specify what the result of the check should be: Uncertain, Error or Success;
- ◆ **Command Time-out** – Number of milliseconds before the command will time-out.

Note: The Remote Command check installs a service on the remote computer in order to execute the command. This service is called 'ActiveXperts Remote Command service'; the associated executable name is 'AxRemSvc.exe'.

The service is uninstalled after the check has completed and is re-installed once the check is processed again.

▼ Scheduled Task

With the Scheduled Task check, one can check if a scheduled task has completed successfully or not. A Scheduled Task check can only be applied to a task that should run today. I.e. you cannot check the completion of a task that ran – for instance – yesterday.

A Scheduled Task check requires the following parameters:

- ◆ **Scheduled Task Log File** – the fully qualified path name to the Scheduled Task Log File (SchedLgU.txt), in UNC format; for instance:
`\\Server01\C$\Windows\Tasks\SchedLgU.txt`
 Please note that this file is hidden in the Windows Explorer. Use a command prompt and type `DIR C:\WINDOWS\TASKS` to list the file;
- ◆ **Job Name** – Job name, as it appears in the SchedLogU.txt file. For instance, job name should be `mytask.bat` according to the following log entry:

```
"mytask.job" (mytask.bat)
Finished 1/19/2006 1:43:00 PM
Result: The task completed with an exit code of (0).
```
- ◆ **Completed Keyword** – The keyword that determines the completion of a scheduled task. For many servers, the keyword will be `Finished`. However, the keyword can be different on non-English Operating Systems you are monitoring;
- ◆ **Today's Date Format** – The string that determines the date format used in the Scheduled Task Log File. Note that your network servers can use different time formats. For that reason, you must specify the date format, so Network Monitor will be able to find the log entries that match the day of today. Default format: `mm/dd/yyyy`, i.e. month (2 digits), day (2 digits), year (4 digits), separated by a '/';
- ◆ **Match Result** – The string that indicates a successful/unsuccessful completion of the task. A successful completion is usually determined by the following string:

```
Result: The task completed with an exit code of (0);
```

 An unsuccessful completion is usually determined by the following string:

```
Result: The task completed with an exit code of (1);
```

 Note that the string can be different on non-English platforms and on legacy (e.g. Windows NT 4) platforms;
- ◆ **If pattern matched, result is** – Indicates the result of the check if pattern is matched: Success or Error.

▼ Service

Service monitoring involves a probe that returns the status of a service. ActiveXperts Network Monitor monitors services on local- and remote computers by checking if the status equals "Running". If so, the server is running fine, otherwise it's not.

A Service check requires the following parameters:

- ◆ **Computer** – The host name or the IP address of the computer you want to monitor;
- ◆ **Service** – The Windows service name. You can either the 'friendly name' (as it appears in the Control Panel) or the 'short name' (the registry key name in the `HKLM\System\CurrentControlSet\Services` registry hive);

- ◆ **Must run / Must not run** – Determines success or error of the check. If the service should NOT be running, select 'Must not run', otherwise select 'Must run';
- ◆ **Credentials** – Select alternate Windows credentials if necessary.

▼ VBScript

ActiveXperts Network Monitor provides a programming interface to IT administrators. VBScript is the standard scripting language in ActiveXperts Network Monitor product. VBScript is the most popular scripting language in Windows environments.

A VBScript check requires the following parameters:

- ◆ **File** – Name of the VBScript file. The script should contain a function as specified in the Function name field. This function should return True (-1) on success, False (0) on error or Unknown (1) in case the results is not known;
- ◆ **Function** – The function that should be called by ActiveXperts Network Monitor. This function should return True (-1) on success, False (0) on error or Unknown (1) in case the result is not known;
- ◆ **Parameter1** – 1st argument of the function (optional);
- ◆ **Parameter2** – 2nd argument of the function (optional);
- ◆ **Parameter3** – 3rd argument of the function (optional);
- ◆ **Parameter4** – 4th argument of the function (optional);
- ◆ **Parameter5** – 5th argument of the function (optional);
- ◆ **Parameter6** – 6th argument of the function (optional);
- ◆ **Advanced Settings:Time-out** – You can specify a time-out for a VBScript check. If the script takes longer than the time-out (in seconds), the function is aborted and an 'Unknown' result is reported. By default, there's no time-out used;
- ◆ **Advanced Settings:Block script after a bad operation** – If a script crashes, for instance because of bad programming, you can block the script so that it will be executed the next time. By default, this option is enabled.

Visit www.activexperts.com/support/activmonitor/online/vbscript/ for detailed information on writing custom VBScript checks.

4.7.3 Linux / Unix checks

▼ SSH Shell Script

SSH Secure Shell allows secure network services over an insecure network, such as the Internet. With SSH, ActiveXperts Network Monitor can login onto a remote machine running the SSH daemon, and execute a command or shell script. ActiveXperts Network Monitor requires the output (i.e. StdOut) to be formatted according to the following syntax:

```
[SUCCESS | ERROR | UNCERTAIN]: { <explanation> } { DATA:<value>}
```

The <explanation> field is displayed in the 'Last Response' column in the Manager application. The <value> field is displayed in the 'Data' column in the Manager application.

Samples:

```
ERROR: Free Disk space is less than 40 GB DATA:34
SUCCESS: Daemon 'LPD' is running
```


To allow clients (incl. ActiveXperts Network Monitor) to run a shell script on Linux/Unix machine using SSH, the following pre-conditions must be met:

- ◆ The remote Linux machine must have the SSH daemon running;
- ◆ The client must have an entry in the `host.allowed` configuration file;
- ◆ The shell script must be copied to the Linux machine first, i.e. it cannot be launched from a Windows machine.

An SSH Shell Script check requires the following parameters:

- ◆ **Remote Host** – Host name or IP address of the remote Linux/Unix host;
- ◆ **Port** – TCP port used for SSH on the remote host. Default port is 22;
- ◆ **SSH Command** – Specifies the command to run on the remote host;
- ◆ **Script Time-out** – Specifies the maximum number of milliseconds to wait for completion of the script; if the script takes longer, it will be terminated. Default value: 5000 milliseconds;
- ◆ **Account** – Account used to authenticate to the remote host;
- ◆ **Password** – Password used to authenticate to the remote host. If you use a Private Key File to authenticate, you can leave the 'Password' field blank;
- ◆ **Private Key File** – Private Key File used to authenticate to the remote host. If you use a Password file to authenticate, you can leave the 'Private Key File' field blank;
- ◆ **If StdErr is not empty, the result will be** – If there's an error in the script, you can handle this error and specify what the result of the check should be: Uncertain, Error or Success.

▼ RSH Shell Script

RSH is a client process that opens connections to an rsh daemon; it sends a command to execute on the remote server and retrieves its output, both stdout and stderr. The connection is established on standard port 514 (tcp port for the shell/cmd protocol). ActiveXperts Network Monitor requires the output (i.e. StdOut) to be formatted according to the following syntax:

```
[SUCCESS | ERROR | UNCERTAIN]: { <explanation> } { DATA:<value>}
```

The `<explanation>` field is displayed in the 'Last Response' column in the Manager application. The `<value>` field is displayed in the 'Data' column in the Manager application.

Samples:

```
ERROR: Free Disk space is less than 40 GB DATA:34
SUCCESS: Daemon 'LPD' is running
```

To allow clients (incl. ActiveXperts Network Monitor) to run a shell script on Linux/Unix machine using RSH, the following pre-conditions must be met:

- ◆ The remote Linux/Unix machine must have the RSH daemon running;
- ◆ The remote Linux/Unix must have an entry in its `.RHOSTS` file for the computer where the ActiveXperts Network Monitor service is running on; this entry must include two values: the host name of the ActiveXperts Network Monitor server and the username to use.

A RSH Shell Script check requires the following parameters:

- ◆ **Remote Host** – Host name or IP address of the remote Linux/Unix host;
- ◆ **RSH Username** – The username to use on the remote host. If not specified, the service account name will be used. The value must be configured in the `.RHOSTS` file on the remote host;
- ◆ **RSH Command** – Specifies the command to run on the remote host;

- ◆ **Script Time-out** – Specifies the maximum number of milliseconds to wait for completion of the script; if the script takes longer, it will be terminated. Default value: 5000 milliseconds;
- ◆ **If StdErr is not empty, the result will be** – If there's an error in the script, you can handle this error and specify what the result of the check should be: Uncertain, Error or Success.

4.7.4 Database checks

▼ Database Query (Generic)

ActiveXperts Network Monitor uses OLE DB (also known as ADO) to check availability of databases.

OLE DB (sometimes written as OLEDB or OLE-DB) is an API for accessing different types of data stores in a uniform manner, including: MS SQL, MS Access, Oracle, MySQL and more.

The Database Query check requires the following parameters:

- ◆ **OLE DB (ADO) Connection String** – The OLE DB connection string, for instance:
`DRIVER=Microsoft Access Driver (*.mdb);DBQ=\\SERVER03\Public\Northwind.mdb`
 You can use a password in this connections string. To hide the password, you can use the `<%PASSWORD%>` placeholder. When using this placeholder, ActiveXperts will automatically substitute this placeholder with the 'Password' field described below;
- ◆ **Password** – This is the password string (shown as asterisks) that will substitute the `<%PASSWORD%>` field described above;
- ◆ **Database Query** – The database query. The result of the check is determined by the result of this query;
- ◆ **Match Field** – The field that will be matched to determine the result of the check;
- ◆ **Type** – Type of field to be checked;
- ◆ **Field must be Equal To / Not Equal To / ...** – Operator used to determine the result of the check;

You can use an AND/OR operator to create an advanced condition.

Note: To check query results, you should use the custom VBScript database check. This check can be fully customized to meet your exact requirements. For instance, you can build complex queries, and analyze the query output.
 To create a new VBScript based database check, select 'New Monitoring Check (VBScript)' from the Monitor menu, and choose `Database.vbs`. Edit `Database.vbs` to meet your requirements.

▼ ODBC Database

ActiveXperts Network Monitor uses ODBC to check availability of a variety of databases. Most major database systems support ODBC, such as: Microsoft SQL Server, Microsoft Access, Microsoft Excel, Oracle, FoxPro, Paradox, SyBase, Informix, OpenIngres, InterBase, Progress, IBM LANDP, DB2 and AS/400.

You must configure ODBC (from the Control Panel on the server where ActiveXperts Network Monitor is running on) before ActiveXperts Network Monitor can check ODBC compliant databases.

An ODBC check requires the following parameters:

- ◆ **ODBC DSN Name** – the ODBC DSN (Data Source Name). This DSN entry must be configured on the server where the ActiveXperts Network Monitor service is running;

- ◆ **Username/Login** – credentials required to access the database;
- ◆ **Password** – credentials required to access the database.

ActiveXperts Network Monitor also provides Oracle checks based on SQLNet, like TNSPing and logon/logoff through SQLNet.

Note: The 'ADO / OLE/DB' check requires fewer configurations and is usually faster. As a result, it is the preferred way to check database, unless the database doesn't ship with an OLE DB driver.

▼ Oracle Database

ActiveXperts Network Monitor uses SQL*Net to monitor Oracle servers for availability. The role of SQL*Net is to establish and maintain a connection between the client application and the server and exchange messages between them.

SQL*Net is a software layer that is required to communicate between Oracle clients and servers. It provides both client-server and server-server communications across any network. It enables client tools to access, modify, share, and store data on Oracle servers over a Network.

The communication between client applications and servers takes place across one or more networks, and is referred to as client/server communication.

ActiveXperts Network Monitor has two SQL*Net based checks for Oracle:

- ◆ TNSPing check;
- ◆ Logon/logoff to a database using username and password for that database.

A Database-Oracle TNSPing check requires the following parameters:

- ◆ **Server TNS name** – TNS name of the Oracle database.

A Database-Oracle Logon/Logoff check requires the following parameters:

- ◆ **Server TNS name** – TNS name of the Oracle database;
- ◆ **Username/Login** – credentials required to access the database;
- ◆ **Password** – credentials required to access the database.

4.7.5 Environmental checks

▼ Temperature

ActiveXperts Network Monitor requires an Environmental Monitor device from [Sensatronics](#) to monitor temperature. By using their server room temperature monitor in your data center design, you are taking a proactive approach in datacenter management. A managed environment can reduce IT server, storage and network outages by 50% or more.

ActiveXperts Network Monitor supports the following Sensatronics models to monitor temperature:

- ◆ Model Senturion (capable of monitoring temperature, humidity, wetness, power, light, motion, smoke, door, resistance, switch);
- ◆ Model EM1 (capable of monitoring temperature, humidity and wetness);
- ◆ Model CM16;
- ◆ Model E16;
- ◆ Model E8;

- ◆ Model E4;
- ◆ Model U16;
- ◆ Model U4.

A Temperature check requires the following parameters:

- ◆ **Host** – The host name or IP address of the network interface of the monitoring device;
- ◆ **Monitor Probe** – Monitor different temperature locations, referred as 'Probe';
- ◆ **Unit** – Select the preferred unit: Fahrenheit, Celsius, Kelvin or Rankine;
- ◆ **Minimum** – Minimum allowed temperature, in Fahrenheit or Celsius;
- ◆ **Maximum** – Maximum allowed temperature, in Fahrenheit or Celsius;
- ◆ **Enable Logging** – Allows you to log all probes.

Data data can be logged to an ASCII log file or to an OLE DB (ADO) compliant database like MS Access or MS SQL.

▼ Humidity

ActiveXperts Network Monitor requires an Environmental Monitor device from [Sensatronics](#) to monitor humidity.

ActiveXperts Network Monitor supports the following Sensatronics models to monitor humidity:

- ◆ Model Senturion (capable of monitoring temperature, humidity, wetness, power, light, motion, smoke, door, resistance, switch);
- ◆ Model EM1 (capable of monitoring temperature, humidity and wetness).

A Humidity check requires the following parameters:

- ◆ **Host** – The host name or IP address of the network interface of the monitoring device;
- ◆ **Monitor Probe** – Monitor different locations, referred to as 'Probe';
- ◆ **Minimum** – Minimum allowed humidity (%);
- ◆ **Maximum** – Maximum allowed humidity (%);
- ◆ **Enable Logging** – Allows you to log all probes.

Data can be logged to an ASCII log file or to an OLE DB (ADO) compliant database like MS Access or MS SQL.

▼ Wetness

ActiveXperts Network Monitor requires an Environmental Monitor device from [Sensatronics](#) to monitor humidity.

ActiveXperts Network Monitor supports the following Sensatronics models to monitor wetness:

- ◆ Model Senturion (capable of monitoring temperature, humidity, wetness, power, light, motion, smoke, door, resistance, switch);
- ◆ Model EM1 (capable of monitoring temperature, humidity and wetness).

A Wetness check requires the following parameters:

- ◆ **Host** – The host name or IP address of the network interface of the monitoring device;
- ◆ **Monitor Probe** – Monitor different locations, referred to as 'Probe';
- ◆ **Minimum** – Minimum allowed wetness;
- ◆ **Maximum** – Maximum allowed wetness;

- ◆ **Enable Logging** – Allows you to log all probes.

Data can be logged to an ASCII log file or to an OLE DB (ADO) compliant database like MS Access or MS SQL.

▼ **Power, Light, Motion, Smoke, Door, Resistance, Switch checks**

ActiveXperts Network Monitor requires the [Sensatronics Senturion](#) device to monitor power, light, motion, smoke, door, resistance or switch.

Such check requires the following parameters:

- ◆ **Host** – The host name or IP address of the network interface of the monitoring device;
- ◆ **Monitor Probe** – Monitor different locations, referred to as 'Probe';
- ◆ **Minimum** – Minimum allowed;
- ◆ **Maximum** – Maximum allowed;
- ◆ **Enable Logging** – Allows you to log all probes.

Data can be logged to an ASCII log file or to an OLE DB (ADO) compliant database like MS Access or MS SQL.

4.7.6 Miscellaneous checks

▼ **Serial Device check**

ActiveXperts Network Monitor allows you to query a serial device (e.g. a modem, a weight indicator, etc.) and analyze the response. The device must have a serial port interface, for instance an RS-232 interface. USB devices are also supported, but only if the device ships with a driver to emulate a serial port.

A Serial Device check requires the following parameters:

- ◆ **Device** – Device driver to use. You can either use a Windows telephony device (recommended) or a physical COM port (directly);
- ◆ **Flow Control** – Select the type of flow control to use. The following values are valid: Default, None, Hardware, Hardware+Software. You can only select 'Flow Control' if 'Device' is set to a direct port (i.e. not a TAPI device);
- ◆ **Baudrate** – Select the baudrate (port speed). You can only select 'Baudrate' if 'Device' is set to a direct port (i.e. not a TAPI device);
- ◆ **Send command when connected** – As soon as connection is established, send a command;
- ◆ **Response must include string** – Expected response;
- ◆ **Time-out** – Number of milliseconds before the check stop reading information from the device.

▼ **Users & Groups**

ActiveXperts Network Monitor monitors groups and group membership. In case of unexpected members in certain groups (for instance: unexpected Domain Admins members), it'll notify the network administrators.

ActiveXperts Network Monitor checks different kinds of Directory Services, for instance: Active Directory, or Novell NDS.

You can configure ActiveXperts Network Monitor to check user accounts (locked out, disabled, etc.), groups, group membership, organizational units, and so on.

The User/Group Membership check requires the following parameters:

- ◆ **Domain** – The Active Directory domain. In case you want to monitor a stand-alone server (i.e. a server not member of a domain), you can enter the computer name;
- ◆ **Group** – The group name to the Active Directory group you want to check, like: Domain Admins;
- ◆ **Users** – Specify the names of the users that are allowed in the specified group. If the groups appears to have members who are not entered in this 'Users' field, the check will fail.

4.8. Writing your own monitoring checks using VBScript

ActiveXperts Network Monitor contains a comprehensive set of built-in monitoring checks. The product is designed to let operators write their own monitoring checks and use them in the product. ActiveXperts uses VBScript because it is the most popular scripting language in Windows environments.

ActiveXperts ships with a collection of cooked VBScript files and routines. These scripts are located in the `Scripts\Monitor` folder, and can be used out of the box. Feel free to modify these scripts.

VBScript check routines should return one of the following values:

- ◆ **-1 (True)**; Return -1 in case the check is successful. For instance, if your function checks the existence of a certain directory, and it does exist, then return -1;
- ◆ **0 (False)**; Return 0 in case the check is not successful. For instance, if your function checks the existence of a certain directory, and it does not exist, then return 0;
- ◆ **1 (Unknown)**; Return 1 in case the check cannot determine True or False. For instance, if your function checks the existence of a certain directory on a server, but it cannot find the server at all (for instance because the computer is down), return 1;

Keep the following in mind when writing a new VBScript function:

- ◆ The routine must be a `Function`, not a `Sub`;
- ◆ The `Function` must return `True (-1)`, `False (0)` or `Unknown (1)`;
- ◆ The `SYSEXPLANATION` and `SYSDATA` variables must be declared (e.g. 'Dimmed') because they are used internally by ActiveXperts Network Monitor;
- ◆ Use the `SYSEXPLANATION` system variable to add your own explanation to the result of the function; this `SYSEXPLANATION` is shown in the client program each time the check is made;
- ◆ Use the `SYSDATA` system variable to store any relevant data, if any. This data field is also shown in the Manager ('Data' column) and is also written to the log files;

Function template:

```
Const retValUnknown = 1
Dim SYSDATA, SYSEXPLANATION

Function Foo( var1, var2, ..., varn )
```

```

If( Not Pre-condition ) Then
    SYSEXPLANANTION = "Unable to determine..."
    Foo = retvalUnknown
Else
    If( condition ) Then
        SYSEXPLANANTION = "Yes it is true because ..."
        SYSDATA = 5
        Foo = True
    Else
        SYSEXPLANANTION = "No it's not true because ..."
        SYSDATA = 6
        Foo = False
    End If
End If
End Function

```

To add a VBScript check:

- ◆ From the **Monitor** menu, choose **New Monitoring Check (VBScript)...**;
- ◆ Select a **VBScript File** and a **VBScript function**;
- ◆ Enter the required parameters and press **OK**.

To create a new VBScript file, choose **Create New File...** from the **File selection box** and a new file will be created.

To create a new function in a VBScript file, choose **Add New Function...** from the **Function selection box** and a new function will be written.

▼ WMI (Windows Management Instrumentation)

If you plan to write check routines based on WMI (Windows Management Instrumentation), be sure you have WMI installed on the ActiveXperts Network Monitor server and on the server that you want to monitor.

WMI is part of the Windows 2008/Vista/2003/2000/XP operating system by default; For WMI for Windows NT4/98/ME, please check the Microsoft website; WMI is available for free.

ActiveXperts has collected more than a hundred WMI samples. You can use these samples as a base for your new check routines. You can find these samples at www.activexperts.com/activmonitor/windowsmanagement/wmi/samples.

▼ ADSI (Active Directory Service Interfaces)

If you plan to write check routines based on ADSI (Active Directory Service Interfaces), be sure you have ADSI installed on the ActiveXperts Network Monitor server and on the server that you want to monitor. ADSI allow you to access not only Windows 2000 Active Directory, but also NT4 User information from the SAM database, and other User Databases like Novell Bindery and so on.

ADSI is part of the Windows 2000 operating system; it's not part of NT4. For NT4, please check the Microsoft website; ADSI is available for free.

ActiveXperts provides some useful ADSI scripts on their website, at www.activexperts.com/activmonitor/windowsmanagement/adsi/samples. You can use these samples as a base for check routines that you write yourself.

▼ VBScript troubleshooting

It's recommended to write and test a custom script as a batch job first, before integrating the script in the Network Monitor software. It is important to write bug-free scripts; a script that is poorly written may block all VBScript based checks at the end. ActiveXperts Network Monitor has a multi-threaded engine, and is capable of processing eight VBScript checks simultaneously. However, when all VBScript threads are blocked, there's no way the Network Monitor can check other VBScript based checks.

General VBScript Guidelines:

1. Location of the script

The batch script must be located in the ActiveXperts Network Monitor installation directory or one of its sub-directories;

2. Use a batch script to test the script

Before integrating the script in the Network Monitor software, test it as a batch job first.

Example:

```
Option Explicit
Const retValUnknown = 1
Dim SYSDATA, SYSEXPLANATION

Function IsWeekend()
    If WeekDay( Date() ) = VBSaturday or WeekDay( Date() ) = VBSunday Then
        SYSEXPLANATION = "Yes, weekend"
        IsWeekend = True
    Else
        SYSEXPLANATION = "No, no weekend"
        IsWeekend = False
    End If
End Function

Wscript.Echo "IsWeekend: " & IsWeekend() ' Use Wscript ONLY for testing
```

(NOTE: the piece of code in green is the code that will be copied to the Network Monitor script when tested well)

Save this file as a .vbs file, for instance: test.vbs.

Then, run it from the command-line like this:

```
CSCRIPT TEST.VBS
```

3. Don't use WScript objects in your scripts

Any commands and functions related to a console or User Interface should be avoided. Keep in mind that the Network Monitor Engine runs as a service, and has no user interface. Message boxes and console output statements may lead to undesirable results. Some objects will not work in Network Monitor:

- ◆ Wscript object;
- ◆ WshArguments object;
- ◆ WshEnvironment;
- ◆ WshNamed;
- ◆ WshNetwork;
- ◆ WshRemote and WshRemoteError;
- ◆ WshScriptExec

- ◆ WshShell
- ◆ WshSpecialFolders;
- ◆ WshUnnamed;
- ◆ WshUrlShortcut.

Also, avoid functions that display a dialog box, like InputBox.

4. Using the ActiveXperts VBScript debugger object

ActiveXperts Network Monitor includes a debug control to print debug information to a log file while the Network Monitor Engine interpreter runs the script. The debug control is called `ActiveXperts.VbDebugger`.

`ActiveXperts.VbDebugger` has the following **properties**:

- ◆ `DebugFile` – the name of the debug output file. The path of the file must be a valid path. If the file does not exist, the file will be created.

`ActiveXperts.VbDebugger` has the following **functions**:

- ◆ `ClearDebugFile` – this function creates a new, empty `DebugFile`. Use it to clear debug output from a previous debug session; The function has no parameters;
- ◆ `Write` – this function writes a piece of text to the `DebugFile`. The function requires one parameter: the string to write to the file. If you want a newline at the end, you must pass it manually yourself as part of the parameter, or use the `WriteLine` function;
- ◆ `WriteLine` – this function writes a piece of text to the `DebugFile`, including a newline at the end. The function requires one parameter: the string to write to the file;
- ◆ `Sleep` – this function will hold the script for some milliseconds. The function requires one parameter: the number of milliseconds.

The following sample shows how to use the debug control:

```
Function IsWeekend()
    Set objDebugger = CreateObject( "ActiveXperts.VbDebugger" )
    objDebugger.DebugFile = "c:\temp\debug.txt"
    objDebugger.ClearDebugFile ' Clear the file if desired
    objDebugger.Write "Function WeekDay will be called now..." & vbCrLf
    If WeekDay( Date() ) = VBSaturday or WeekDay( Date() ) = VBSunday Then
        SYSEXPLANATION = "Yes, weekend"
        IsWeekend = True
    Else
        SYSEXPLANATION = "No, no weekend"
        IsWeekend = False
    End If
    objDebugger.Sleep 3000 ' Hold the script for three seconds
    objDebugger.Write "Exit IsWeekend" & vbCrLf
End Function
```

▼ Online ActiveXperts VBScript Guidelines

Visit www.activexperts.com/support/activmonitor/online/vbscript/ for detailed information on writing custom VBScript checks. It contains detailed information about writing custom scripts, describes the debugger and contains various samples.

4.9. Writing your own monitoring checks using a Linux/Unix Shell Script

The Secure Shell Script (SSH) check allows you to login to a Linux/Unix host and run a shell script in a secure way. There are two ways to login: using an account and a password, or using an account and a private key file.

ActiveXperts Network Monitor requires the output (i.e. StdOut) to be formatted according to the following syntax:

```
[SUCCESS | ERROR | UNCERTAIN]: { <explanation> } { DATA:<value>}
```

The <explanation> field is displayed in the 'Last Response' column in the Manager application. The <value> field is displayed in the 'Data' column in the Manager application.

Samples:

```
ERROR: Free Disk space is less than 40 GB DATA:34
SUCCESS: Daemon 'LPD' is running
```

Sample Shell Script to check directory existence:

```
#!/bin/sh

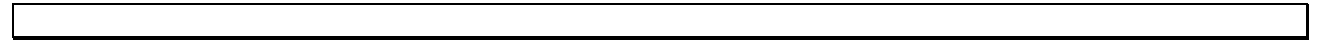
# Macro definitions
FREE=`free -m | awk '/^Mem:/ { printf( "%s\n", $4 ); }`
USED=`free -m | awk '/^Mem:/ { printf( "%s\n", $3 ); }`

# Validate number of arguments
if [ $# -ne 2 ] ; then
    echo "UNCERTAIN: Too few arguments Usage: memory <free>|<usage> <size>";
    exit 1;
fi

# Validate arguments
if [ $1 != "free" ] && [ $1 != "used" ]; then
    echo "ERROR: Wrong parameters entered DATA:0";
fi

# Check free memory
if [ $1 == "free" ] ; then
    if [ $FREE -gt $2 ]||[ $FREE == $2 ] ; then
        echo "SUCCESS: Free memory is [$FREE MB], minimum required=[$2 MB]
DATA:$FREE";
    else
        echo "ERROR: Free memory is [$FREE MB], minimum required=[$2 MB]
DATA:$FREE";
    fi
fi

# Check used memory
if [ $1 == "used" ] ; then
    if [ $USED -lt $2 ]||[ $USED == $2 ] ; then
        echo "SUCCESS: Used memory is [$FREE MB], maximum allowed=[$2 MB]
DATA:$FREE";
    else
        echo "ERROR: Used memory is [$FREE MB], maximum allowed=[$2 MB]
DATA:$FREE";
    fi
fi
```



ActiveXperts Network Monitor ships with a selection of monitoring checks implemented as shell scripts. These script are located in the following directory: `\Scripts\Monitor(Linux)`

5. Managing Folders

In ActiveXperts Network Monitor, all checks are organized into folders. Folders can be used in the Web Interface (to show only checks located in a particular folder), in Reports (to create reports of check within particular folders) and in Dependency relationships.

5.1. Adding a new Folder

To add a new folder:

- ◆ On the **Monitor menu**, choose **New Folder**;
- ◆ In the Name field, type the name of the new folder.

5.2. Editing a Folder

To edit a folder:

- ◆ Select the **Folder** you want to edit;
- ◆ Choose **Properties** from the **Monitor menu**;
- ◆ Type a new name for the folder.

5.3. Deleting a Folder

To quickly delete a folder, select the appropriate folder and click **Delete**  on the toolbar.

To delete a folder:

- ◆ Select the **Folder** you want to delete;
- ◆ Choose **Delete** from the **Monitor menu**. When you delete a folder, all check routines and sub-folders in the folder tree will also be deleted.

6. Web Interface

6.1. Introduction

The ActiveXperts Network Monitor Web Interface is a collection of web pages, also called Web Views.

Web Views are web pages, generated by the Network Monitor Engine, to provide a user interface to users who do not have the Network Monitor Manager installed. An Internet Browser can be used to view the status of the network.

Web Views are based on XML/XSL technology. Web Views require Internet Explorer 6.x or higher, or any other web browser that is capable of parsing XML files.

XML stands for Extensible Markup Language. It's a markup language much like HTML. The big difference is, that XML was designed to describe data; HTML was designed to display data. XML tags are not predefined. ActiveXperts Network Monitor defines its own tags for their Web Views.

The World Wide Web Consortium (W3C) started to develop XSL because there was a need for an XML based Style sheet Language.

XSL can transform XML into HTML, filter and sort XML data, define parts of an XML document, format XML data based on the data value, and more. This is exactly how Web Views work in ActiveXperts Network Monitor.

It is important to understand that XML is not a replacement for HTML; XML is a cross-platform, software and hardware independent tool for transmitting information.

The tags used to mark up HTML documents and the structure of HTML documents are predefined. The author of HTML documents can only use tags that are defined in the HTML standard (like `<p>`, `<h1>`, etc.). XML allows ActiveXperts Network Monitor to define his own tags and his own document structure; the tags are described in the section 'XML Tags in Web Views' in this section.

Web Views are preferred over the ActiveXperts Network Monitor Manager application when:

- ◆ User requires read-only access to ActiveXperts Network Monitor;
- ◆ User monitors remotely through a firewall; Web Views only requires access on one port (for instance, port 80);
- ◆ User monitors multiple networks, with different Network Monitor configurations;
- ◆ User needs access to ActiveXperts Network Monitor from any place in the organization; for instance, the HelpDesk staff can access Network Monitor from any workstations in the organization;
- ◆ User is using a thin-client box, like a Windows CE based Wyse Terminal;

6.2. Using the Web Interface

The ActiveXperts Network Monitor software is delivered with a pre-defined set of Web Views. To view these Web Views:

- ◆ In the **Tools menu**, point to **Web Interface** and select **Web Interface (default page)**;
- ◆ The Web Interface default page is launched, where you can click on a particular Web View.

Note: You need an XML capable browser to make use of the Web Interface, like Internet Explorer 6.x or Firefox 1.5.
XSL in Internet Explorer 5 is NOT compatible with the official W3C XSL Recommendation. When Internet Explorer 5.0 was released in March 1999, the XSLT standard was still a W3C Working Draft. Since the final W3C XSL Recommendation is different from the Working Draft, the support for XSL in IE 5 is not 100% compatible with the official XSLT Recommendation. This restriction applies to both IE 5.0 and IE 5.5.

6.3. Customizing the Web Interface

▼ Web Interface Configuration Tool

Use the Web Interface Configuration Tool to customize the Web Interface. Use it also to create, modify or delete Web Views.

To launch the Web Interface Configuration Tool:

- ◆ In the **Tools menu**, point to **Web Interface** and select **Web Interface Configuration Tool**;

With the Web Interface Configuration Tool, you can configure the following items:

- ◆ **Enable Web Interface** – by default, Web Views are enabled. Disabling the web interface will slightly improve the performance of the Network Monitor service;
- ◆ **Generate Web Views every x seconds** – Web Views refresh rate;
- ◆ **Installed Web Views** - Each Web View consist of one XML file and a related XSL file. The XSL is the Style Sheet, and is not generated by the software; you can customize the Web View by modifying the XSL file.
Each XML file is generated by the Network Monitor service; it will contain all monitoring results, and has a reference to the corresponding XSL file.

You can add, delete and edit Web Views at any time. A restart of the Network Monitor service is not required.

▼ Publishing the Web Interface using IIS

It's recommended to publish the XML pages through IIS, but they can also accessed directly by UNC path. You can manually configure IIS to provide the ActiveXperts Network Monitor pages in the following way:

- ◆ Click **Start**, point to **Administrative Tools** and click on **Internet Information Services (IIS) Manager** to open the **IIS Management Console**;
- ◆ Create a new web site by choosing **New Web Site**;
- ◆ Provide a description and port number;
- ◆ Provide a path name. Either use a local path (like `C:\Program Files\ActiveXperts\Network Monitor\Web`) or an UNC path (like `\\SERVER01\AXNetMon\Web`);
- ◆ Finish the web site creation wizard. Then choose Web Site 'Properties', select the 'Documents' tab and add the file, for instance `WebView1.Xml`;

▼ Web Interface XML tags

Appendix B: “Web Interface XML Tags” describes the XML tags in the web interface XML pages.

7. Report Module

7.1. Introduction

With the ActiveXperts Report Module, you can create reports over a specified period of time, Reports can either be run ad hoc, or they can be scheduled from the Windows Task Scheduler, which will run them automatically, periodically (, e.g. daily, weekly or monthly). When a report is run from a schedule, the report results can be sent to a list of e-mail recipients.

Report Data is stored in an MS Access database by default, but can be migrated to an MS SQL database at any time. The MS Access report database is called `REPORTDATA.MDB` and is located in the `<INSTALL-DIR>\Logs\` directory.

The ActiveXperts Reports Module features the following:

- ◆ Availability Reports. These reports contain reports aggregate fields, such as total up-time, total down-time etc. Aggregate fields are shown as absolute values (e.g. days, hours, minutes) as well as relative (percentage) values;
- ◆ Detail Reports. These reports show all state changes, including reason for the state change and amount of time it remained in that particular state;
- ◆ Filters - A comprehensive range of filters which can be applied to reports ensures that your reports only return the data you require. The filters available include checks, folders and results;
- ◆ The Report Module offers different ways in which to specify the time period for which a report is to be run. A report can be run between specific dates and times or for a specific number of days, weeks, months or years from the current date or from the previous calendar period.
- ◆ Create reports interactively (ad-hoc), from the command line or scheduled;
- ◆ Dedicated tool ('Report Configuration Tool') to define new report templates;
- ◆ Supported formats: XML, XML/XSL, HTML and CSV;
- ◆ Report distribution via e-mail. Scheduled Reports can be configured so that the report results are sent to a list of email recipients once the report has been run. Daily, Weekly and Monthly recurring schedules can be set up and reports attached to them to be run periodically with the results being distributed to a list of email recipients. In this way, ActiveXperts Network Monitor can be configured so that all reports are scheduled and ran automatically, with the report results being distributed automatically, so that no user input is required once the system has been set up.

7.2. Report Definition Files (*.rep)

To create a new report, you must always select a Report Definition file (`.rep`). This definition file describes the properties of a report, including:

- ◆ Type of report, i.e. a 'detail' report or an 'availability' report. A 'detail' report shows the length of time the servers were in a particular state; an 'availability' report provides overall availability information of the servers;
- ◆ Which checks (or groups of checks) should be included in the report;
- ◆ Date ranges, like: today, this month, last 4 weeks, etc.
- ◆ Output format. Supported output formats: XML, XML/XSL, HTML and CSV;

- ◆ Name of the output file. You can use placeholders to use dynamic report file names;
- ◆ Filters; you can filter on Checks, Folders, Check Types, and Results;
- ◆ E-mail recipients.

ActiveXperts Network Monitor ships with a few pre-defined Report Definition file that can be used to create a new report, e.g.:

- ◆ Availability_Day.rep
- ◆ Availability_DayPrev.rep
- ◆ Availability_Month.rep
- ◆ Availability_MonthPrev.rep
- ◆ Detail_Day.rep
- ◆ Detail_DayPrev.rep
- ◆ Detail_Month.rep
- ◆ Detail_MonthPrev.rep

7.3. Creating a new Report manually

▼ Step 1: Launch the Report Generator Wizard

You can launch the Report Generator tool from the Manager: open **Reports** from the **Tools menu** and select **Create New Report....** The Report Generator Wizard starts with a welcome screen. Click **Next** to continue.

▼ Step 2: Select a Report Definition File

You must now select a Report Definition (.rep) file. Such a definition file includes all properties of the new report, including type of report, date ranges, name of the report output file, etc.. You can use one of the pre-installed Report Definition files, but you can use your own Report Definition file. See also Chapter 7.4: "Customizing Reports".

▼ Step 3: Finish

Finally, press **Finish** to create the report.

The report is saved in the <INSTALL-DIR>\Reports directory, with a filename as specified in the Report Definition file.

The results of the report creation are logged in the following file: <INSTALL-DIR>\LOGS\REPORTGENERATOR.LOG

You can choose not to send the report to the e-mail recipients (the check box is only enabled when the Report Definition file contains e-mail recipients).

7.4. Creating a new Report automatically (scheduled)

The ActiveXperts Network Monitor Reports Module allows you to send out reports automatically to a specified list of e-mail recipients. This can be useful for scheduled reports, for instance for reports that run automatically every week or every month.

▼ Step 1 – Configure a Report Definition file with e-mail recipients

To send a report to e-mail recipients from a scheduled job, you must configure the e-mail recipients in the Report Definition (.rep) file.

The ActiveXperts Report Modules uses the same global e-mail settings as the ActiveXperts Network Monitor Manager and the ActiveXperts Network Monitor Service, like: SMTP server, fallback SMTP server (if any), SMTP login credentials (if any), E-mail Address Book, etc. To change global e-mail settings, you must use the ActiveXperts Network Monitor Manager.

To configure e-mail recipients for a Report Definition (.rep) file:

- ◆ Start the **Report Configuration Tool**;
- ◆ Select a Report Definition File from the list, and press the **Edit Selected** button;
- ◆ Select the **E-mail Properties sheet**;
- ◆ Select the **E-mail report checkbox**. You can now edit the e-mail subject and e-mail body, and select the e-mail recipients.

NOTE: It is recommended to use E-mail Distribution Groups (from the E-mail Address Book) rather than individual recipients. With a Distribution Group, you don't need to change the Report Definition file to add/remove a recipient. You just need to modify the Distribution Group's recipient list. Besides that, a Distribution Group can be used by multiple Report Definition files.

▼ Step 2 – Create a test report from the command line (AxRgCmd.exe)

Before you schedule a report using the Task Scheduler, it is recommended to test the report using the command line tool `AxRgCmd.exe`. This command line tool produces the same result as the graphical report tool (`AxRgGui.exe`) described in Chapter 7.2, but does not require any user intervention so it can be run from the Task Scheduler.

To create a new report from the command line:

- ◆ Start a new Command Prompt. You can start the prompt by pointing to **Run** in the **Start menu**, and type: `CMD.EXE`
You can also start a new prompt pointing to **Accessories** from the **All Programs menu**, and then select **Command Prompt**.
- ◆ Change the current directory; set it to the network monitor installation directory. For instance:
`CD "C:\Program Files\ActiveXperts\Network Monitor"`
- ◆ Start the command line program to create a new report. It requires one parameter: the Report Definition File to be used to create the new report. For instance:
`AXRGCMD.EXE /f detail_day.rep`
- ◆ The command line utility will create the report file. The output filename is specified in the Report Definition File. The results of the operations are logged in the following file:
`<INSTALL-DIR>\LOGS\REPORTGENERATOR.LOG`

▼ Step 3 - Schedule a Report using the Task Scheduler

Report creation can be automated by scheduling the creation of a report using the Windows Task Scheduler. Scheduling is often used to create monthly reports and send the report to a specified list of e-mail recipients.

With the Task Scheduler, you can only run the command-line version of the Report Creation Tool (AXRGCMD.EXE). The graphical version (AXRGGUI.EXE) requires user input and is not designed to run from the Task Scheduler.

'Step 3' already described how to use the AxRgCmd.exe tool command line tool. This tool can be used to create a report from the command line using a Report Definition (.rep) file, without user intervention, for example:

For scheduled tasks, it is recommended to make use of a batch file to encapsulate parameters. For instance: C:\Program Files\ActiveXperts\Network Monitor\Report Definitions\BatchJobs\Detail_Day.cmd:

```
@echo off
CD "C:\Program Files\ActiveXperts\Network Monitor\"
AXRGCMD.EXE /f Detail_Day.rep
```

To create a new scheduled report, perform the following steps:

- ◆ Click **Start**, click **Control Panel** and double-click the **Scheduled Tasks icon**;
- ◆ Double-click **Add Scheduled Tasks**. The Scheduled Task Wizard pops up; click **Next** to skip the welcome page;
- ◆ Click the **Browse button** to select a batch job, for instance:
C:\Program Files\ActiveXperts\Network Monitor\Report Definitions\BatchJobs\Detail_Day.cmd
- ◆ Specify a name for this task, and specify the frequency;
- ◆ Specify credentials. It is recommended to use an account that is member of Local Administrator group;
- ◆ Press **Finish** to complete the configuration of the scheduled task.

7.5. Customizing Reports

ActiveXperts' reporting is based on Report Definition Files (.rep). Such a Report Definition file describes the characteristics of a new report, including:

- ◆ Type of report, i.e. a 'detail' report or an 'availability' report;
- ◆ Begin date and end date;
- ◆ Filters;
- ◆ Output format: XML, XML/XSL, HTML or CSV;
- ◆ E-mail recipients;

With the Report Configuration Tool, you can:

- ◆ Create new Report Definition Files;
- ◆ Modify existing Report Definition Files
- ◆ Delete Report Definition Files

To create/modify a Report Definition File:

- ◆ Start the **Report Configuration Tool** by pointing to **Reports** from the **Tools menu**. Select **Report Configuration Tool** to launch the tool.
- ◆ To create a new Report Definition File, click on the Add New button;
- ◆ To modify an existing Report Definition File, select a Report Definition File from the list box and press the **Edit Selected button**.
- ◆ When you create or edit a report, a wizard starts. It will prompt you for all necessary info.

▼ Availability Reports vs. Detail Reports

One of the configurable items in a Report Definition File is the type of report. It can be:

- ◆ Availability Report;
- ◆ Detail Report.

An 'availability' report provides overall availability information of your servers/checks during the nominated date range. You can see uptimes and downtimes, in days, hours, minutes and seconds, and also as percentages. A 'availability' report is used for instance to compare real availability statistics against the SLA requirements.

A 'detail' report provides a detailed list of all state changes during the nominated date range. For each check, you can see exactly when and why it failed, and for how long.

▼ Begin Date and End Date of a report

One of the configurable items in a Report Definition File is the begin date and the end date selection of a report. You can select the absolute begin date and end date, but it is recommended to use a relative begin date and end date. You can select the following relative date selectors:

- ◆ This day;
- ◆ This week;
- ◆ This month;
- ◆ This quarter;
- ◆ Last x days;
- ◆ Last x months;
- ◆ Last x quarters;
- ◆ Last x years.

▼ Output format

One of the configurable items in a Report Definition File is the report output format. ActiveXperts Network Monitor supports four different output formats:

- ◆ XML/XSL – the output format is XML, and the screen layout definition is described in XSL. The XML file is generated automatically by the report generator, and contains a reference to the XSL layout file; the XSL layout file is static and can be modified at any time. The XML/XSL pair can be read by any Internet browser;
- ◆ XML – this output format is supported by many applications. This format is very useful when you want to import the report data into a 3rd party application. But since it has no reference to an XSL file, it has no graphical formatting.
- ◆ HTML – this format can be read by any browser;
- ◆ CSV – this output format is supported by many applications. This format is very useful when you want to import the report data into a 3rd party application.

▼ Output filename

One of the configurable items in a Report Definition File is the report output filename.

You can choose for:

- ◆ Static filename – a fixed filename, without placeholders;
- ◆ Dynamic filename – a variable filename. It has year/month/day placeholder, so its name depends on the date when the report is created.

One of the configurable items in a Report Definition File is the report output filename.

If you use scheduled day/week/month/quarter/year reports, it is recommended to use dynamic filenames. Otherwise, new report files will automatically overwrite older ones, because the report output files have identical names.

With dynamic files, the name of the report file depends on the date it is created. You can use the following placeholders:

- ◆ DD – day notation with leading zero
- ◆ D – day notation without leading zero
- ◆ MM – month notation with leading zero
- ◆ M – month notation without leading zero
- ◆ YYYY – year notation
- ◆ YYY – year notation (3 digits only)
- ◆ YY – year notation (2 digits only)
- ◆ Y – year notation (1 digit only)

Examples:

```
Filename:      DetailReport%MMDDYY%.xml
Date of creation: 20060422
Result:       DetailReport042206.xml
```

```
Filename:      DetailReport%MDYYYY%.xml
Date of creation: 20060422
Result:       DetailReport4222006.xml
```

▼ Filters

You can define filters in your Report Definition File to show only a subset of all checks in your reports.

You can define the following filters:

- ◆ Checks – include all check in your report, or only a subset of all checks;
- ◆ Check Types – include all kinds of checks, or only a subset. You can for instance create a report that only contains ICMP and HTTP checks;
- ◆ Result – include only checks that have a specified result. For instance you can create a report of all checks with result: failed.

▼ E-mail

The ActiveXperts Reports Module allows you to send out reports automatically to a nominated list of e-mail recipients. This is particularly useful for automated reports, where reports are created daily/weekly/monthly, automatically. Recipients are automatically notified of a new report. They just need to click on the URL that is inside the e-mail message.

The ActiveXperts Reports Module makes use of the SMTP settings and E-mail address book of the ActiveXperts Network Monitor configuration. So, it uses the same primary- and secondary SMTP server as used by the ActiveXperts Network Monitor service. You can use the same e-mail distribution groups as used for e-mail alerts.

7.6. Formatting Reports

The HTML- and XML reports are based on an XSL stylesheet to format the report. With the HTML report, the stylesheet is used to create the HTML report. Once the report has been created, you cannot change the format of the produced HTML report. With XML based reports, a link to the XSL stylesheet is included in the XML report. This means that report data and formatting are stored in two separate file, so you can change the format of the XML report at any time.

▼ XML Report Data

Appendix A: “Report Data Format” describes the Report Data of the XML files.

▼ XSL

The ActiveXperts Reports Module allows you to send out reports automatically to a nominated list

By default, all XML/HTML ‘detail’ reports are based on the following XSL stylesheet:

`DetailReport.xsl`

All XML/HTML ‘availability’ reports are based on the following XSL stylesheet:

`AvailabilityReport.xsl`

To change the format of a report, you can either modify the XSL file, or create a new custom XSL file and link the reports to the new XSL file.

To create a new XSL file:

- ◆ Start the **Windows Explorer**;
- ◆ Point to the `<INSTALLDIR>\Report Definitions\StyleSheets` directory;
- ◆ Make a copy of an existing XSL sheet.

To link a report to a new custom XSL file:

- ◆ Start the **Report Configuration Tool** by pointing to **Reports** from the **Tools** menu. Select **Report Configuration Tool** to launch the tool;
- ◆ Change the properties of a Report Definition (.rep) file;
- ◆ In the Output Selection page, select a new XSL file. XSL files are located in the `<INSTALLDIR>\Report Definitions\StyleSheets` directory.

To modify an XSL file:

- ◆ Start the **Windows Explorer**;
- ◆ Point to the `<INSTALLDIR>\Report Definitions\StyleSheets` directory;
- ◆ Select an XSL file and choose **Edit** from the context menu.

To change the format of an HTML or XML report requires basic knowledge of XSL. A good tutorial to XSL can be found here: www.w3schools.com.

▼ Basic XSL statements

Use the `<xsl:for-each>` tag to iterate over a set of checks.

```
<xsl:for-each select="monitor/check">
  ...
  <br><xsl:value-of select="result"/><br>
```



```
</xsl:for-each>
```

The XSL `<xsl:for-each>` element can be used to select every XML element of a specified node set. The `<xsl:value-of>` element can be used to select the value of an XML element and add it to the output stream of the transformation.

Use the `<xsl:sort>` tag to sort a record set.

```
<xsl:for-each select="monitor/check">
  <xsl:sort select="result"/>
  <xsl:sort select="displayname"/>
  ...
</xsl:for-each>
```

To sort output it at the same time, simply add the `<xsl:sort>` sort element inside the for-each element in your XSL file. Use multiple `<xsl:sort>` elements to sort on multiple columns.

Use the `<xsl:if>` tag to use a condition.

```
<xsl:if test="result > 2">
  ...
</xsl:if>
```

To put a conditional if test against the content of the file, simply add an `<xsl:if>` element to your XSL document. The value of the required test attribute contains the expression to be evaluated.

8. Permissions

You can assign the following permissions to users and groups of users:

- ◆ No Access;
- ◆ Read-only;
- ◆ Read-write.

ActiveXperts Network Monitor uses file system permissions to allow/disallow users to use the software.

Only two files/shares are important when dealing with permissions:

- ◆ The ActiveXperts Network Monitor **share**, which must be created to allow Remote Network Monitor Applications. Configure this Share through the Network Monitor Manager application on the machine where the Network Monitor Engine is running;
- ◆ The `CONFIG.MDB` **file** – this single file holds ALL the configuration data and is located in the `<installation directory>\Configuration` directory on the ActiveXperts Network Monitor server;

8.1. No Access

Use the ActiveXperts Network Monitor Share on the ActiveXperts Network Monitor server to assign No Access permissions to users or groups.

By default, the following share permissions are assigned:

Everyone: Full Control

This will allow all users on the network to install the ActiveXperts Network Monitor Manager application and to use the Manager application.

Only assign share permissions to people who are allowed to use ActiveXperts Network Monitor. Always assign Change permissions on the share to people who will use ActiveXperts Network Monitor, even if they only need read-only permission. Change is required to allow read-only users to send control information to the ActiveXperts Network Monitor service, for instance to request to monitor a particular server immediately.

Two scenarios:

Scenario 1: Allow only Domain Admins to use ActiveXperts Network Monitor.

Share permissions: Domain Admins: Change

Scenario2: Allow everyone in the domain except users Joe

Share permissions: Domain Users: Change
Joe: No Access

8.2. Read-only access

Read-only access means, that a user can only view results of the ActiveXperts Network Monitor, but cannot make changes to the configuration.

The `CONFIG.MDB` file plays an important role in assigning read-only permissions. The `CONFIG.MDB` file holds ALL configuration data and is located in the `<INSTALL-DIR>\CFG` directory on the ActiveXperts Network Monitor server;

People who are only allowed to view results of ActiveXperts Network Monitor, should have read-only permissions on the `CONFIG.MDB` file. By having read-only access to the `CONFIG.MDB` file, the user cannot make changes to the configuration.

The ActiveXperts Network Monitor Manager application detects the read-only permissions on the `CONFIG.MDB` and disables certain menu's and commands for the particular user.

Still assign Change permission on the Share for read-only users. Change permission is needed to send control information to the ActiveXperts Network Monitor service.

<u>Scenario:</u>	Allow Domain Admins to configure ActiveXperts Network Monitor and view monitor results, allow all other people to view the monitor results only.	
Share permissions:	Domain Admins:	Change
<code>CONFIG.MDB</code> :	Domain Admins:	Change
	Domain Users:	Read

8.3. Read/write access

Read-write access means, that a user can view and configure ActiveXperts Network Monitor. People, who are allowed to make changes to the ActiveXperts Network Monitor configuration, should have Change permissions on the `CONFIG.MDB` file. By having Change access to the `CONFIG.MDB` file, the user can make changes to the configuration, as well as view the monitor results.

<u>Scenario:</u>	Allow Domain Admins to configure ActiveXperts Network Monitor.	
Share permissions:	Domain Admins:	Change
<code>CONFIG.MDB</code> :	Domain Admins:	Change

9. Tuning the System

9.1. Introduction

The ActiveXperts Network Monitor Engine (a Windows Service) is responsible for monitoring servers, workstations and devices from a central point. It is designed to run multiple checks simultaneously. To do so, it uses so called 'threads'. Multi-threading gives a program the ability to perform several tasks concurrently.

In ActiveXperts Network Monitor, multiple threads are spawned, including:

- ◆ **Dispatcher** - holds the configuration of the software. It has a queue of checks and decides which checks need to be checked. It determines which threads are busy and which threads are not, and passes a check to a thread that is capable of handling that type of check;
- ◆ **Notifications and Reports** - Notifications can be time consuming, and are therefore assigned to threads to do its job. For instance, an SMS message through an SMSC dial-up provider can take up to 90 seconds. A NetPopup notification message to a non-existing NetBIOS recipient can take up to 10 seconds;
- ◆ **Checks** - There are many threads for different checks, to optimize ActiveXperts Network Monitor's monitoring performance. There are threads for ICMP checks, Oracle checks, etc.

The number of threads strongly influences the performance of the ActiveXperts Network Monitor Engine (service). If there are only a few threads, the software will not use much CPU and memory resources, but the throughput of checks may be low. By increasing the number of threads, the throughput will increase. However, too many threads will consume too many system resources together (each thread consumes memory and CPU), decreasing the performance of the Network Monitoring engine dramatically.

It is recommended to have less than 40 threads on an average server. If - for instance - you have a lot of ICMP checks, and only a few VBScript based checks, you can increase performance by configuring a few more ICMP threads and a few less VBScript threads.

On more powerful servers, you can configure more threads.

9.2. Configuring the number of Threads

To configure the number of threads, choose Options from the Tools Menu and select the Advanced tab. Press on the top-most button.

You find all different types of threads. You can change the number of threads that is spawned when the ActiveXperts Network Monitor is started. As a result, changes take affect after you restart the service!

The following threads are used by the network Monitor Engine (service):

- ◆ **Environmental** - Handles environmental related checks: 'Temperature', 'Humidity' and 'Wetness'. Default number of Environmental threads: 2.
- ◆ **ICMP/Ping** - Handles 'ICMP/Ping' checks. Default number of threads: 4;
- ◆ **HTTP** - Handles 'HTTP/HTTPs' checks. Default number of threads: 4;

- ◆ **FTP** - Handles 'FTP' and 'TFTP' checks. Default number of threads: 1;
- ◆ **OLE DB** - Handles generic 'Database' checks, including checks for MS Access and MS SQL. Default number of threads: 2;
- ◆ **Oracle** - Handles 'Oracle' checks. Default number of threads: 1.
IMPORTANT: you can configure only 1 Oracle thread;
- ◆ **Serial Communications** - Handles 'Serial Device' checks. Default number of threads: 1;
- ◆ **SSH** - Handles 'SSH' checks. Default number of threads: 1;
- ◆ **SMTP to POP3** - Handles 'SMTP to POP3' checks. Default number of threads: 1;
- ◆ **SNMP Trap Receiver** - Handles 'SNMP Trap Receive' checks. Default number of threads: 1;
- ◆ **Socket** - Responsible for Winsock related checks: 'TCP', 'POP3', 'SMTP', 'RSH', 'SNMP', 'NTP', 'NNTP', 'Terminal Server', 'IMAP' and 'DNS'. Default number of Socket threads: 4;
- ◆ **VBScript** - Responsible for handling VBScript based checks, including custom VBScript checks. Default number of VBScript threads: 4.
IMPORTANT: you cannot define more than 8 VBScript threads;
- ◆ **Win32** - Responsible for handling the following checks: 'Directory Size', 'Disk Space', 'Service' and 'File Existence'. Default number of Win32 threads: 4;
- ◆ **WMI** - Responsible for handling all WMI based checks: 'CPU', 'Disk Drives', 'Memory', 'Printer', 'Process' and 'Event Log'. Default number of WMI threads: 4.

9.3. Log files

ActiveXperts Network Monitor maintains its own log files. By default, logging is enabled, and is written to the <INSTALL-DIR>\LOGS directory. You can change this directory from the **Options dialog** in the **Tools menu**.

10. Troubleshooting

Visit our website at <http://www.activexperts.com/support/activmonitor> for a complete FAQ list. You can also send an email to our support staff: support@activexperts.com.

11. Purchase and Product Activation

11.1. License Scheme

ActiveXperts Network Monitor licensing options:

- **Small Business License.**
This license allows you to install and use the software on any workstation or server in your organization.
You are allowed to monitor up to 10 IP-devices/workstations/servers inside your organization.
You are not allowed to monitor any device/workstation/server outside your organization, except servers that are on the public internet (for instance: web servers, mail servers, etc.).
You are not allowed to install the software outside your organization or distribute the product as part of your own software.
- **Enterprise license.**
This license allows you to install and use the software on any workstation or server in your organization.
You are allowed to monitor an unlimited number of IP-devices/workstations/servers inside your organization.
You are not allowed to monitor any IP-device/workstation/server in other organizations, except servers that are on the public internet (for instance: web servers, mail servers, etc.).
You are not allowed to install the software outside your organization or distribute the product as part of your own software.
- **Universal License - 5 Organizations.**
This license allows you to install and use the software on any workstation or server in your organization.
You are allowed to monitor an unlimited number of IP-devices/workstations/servers inside your organization.
You are also allowed to monitor an unlimited number of IP-devices/workstations/servers in 5 other organizations.
You are not allowed to distribute the software as part of your own software.
- **Universal License - Unlimited Organizations.**
This license allows you to install and use the software on any workstation or server in your organization.
You are allowed to monitor an unlimited number of IP-devices/workstations/servers inside your organization.
You are also allowed to monitor an unlimited number of IP-devices/workstations/servers in any other organization (unlimited).
You are not allowed to distribute the software as part of your own software.

Please visit:

<http://www.activexperts.com/sales>
to read more about our licensing schemes.

11.2. Purchase

Please visit:

<http://www.activexperts.com/sales>

to read more about how to purchase the product. On this site, you can also find the URL to make an online order.

You can also contact us via email: sales@activexperts.com.

11.3. Product Activation

After you have installed the product, you can use the software for 30 days. All features are available during this period. After 30 days, the Manager application can still be launched, and the service will keep on running. However, you won't be able to (re)start the service anymore.

During the trial period, you can check how many days are left at any time: go to the **Help menu** and select the **About ActiveXperts Network Monitor menu item**. It'll pop up an about dialog, which displays the number of days remaining.

After you purchase the product, you will receive one or more product registration keys. These must be entered by using the ActiveXperts Network Monitor Manager application.

To enter the registration code, go to the **Help menu**, and choose **Registration**. Enter the registration code and press OK.

APPENDIX A: Report Data Format

A.1. XML Availability Reports

To customize 'availability' reports, you need to make changes to the XSL file. Before you can make changes to the XSL file, a little understanding of the XML document is required.

The XML document is the result of the Report Creation Tool (either AXRGGUI.EXE or AXRGCMD.EXE). It has a reference to a static XSL document. This XSL document describes how the XML document should be displayed.

The XML document of a 'availability' report looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="stylesheets\AvailabilityReport.xsl"?>
<monitor>
  <from-secs>1154124000</from-secs>
  <to-secs>1154210399</to-secs>
  <from-date>07/29/2006 12:00:00 AM</from-date>
  <to-date>07/29/2006 11:59:59 PM</to-date>
  <check>
    <id>10288</id>
    <displayname>www.monitortools.com - ICMP Ping</displayname>
    <check>ICMP</check>
    <folder>\</folder>
    <uncertain-secs>0</uncertain-secs>
    <uncertain-hrsmin>000 00:00:00</uncertain-hrsmin>
    <uncertain-pct>0.00</uncertain-pct>
    <success-secs>1829</success-secs>
    <success-hrsmin>000 00:30:29</success-hrsmin>
    <success-pct>2.12</success-pct>
    <failure-secs>0</failure-secs>
    <failure-hrsmin>000 00:00:00</failure-hrsmin>
    <failure-pct>0.00</failure-pct>
    <maintenance-secs>0</maintenance-secs>
    <maintenance-hrsmin>000 00:00:00</maintenance-hrsmin>
    <maintenance-pct>0.00</maintenance-pct>
    <onhold-secs>0</onhold-secs>
    <onhold-hrsmin>000 00:00:00</onhold-hrsmin>
    <onhold-pct>0.00</onhold-pct>
    <depfailure-secs>0</depfailure-secs>
    <depfailure-hrsmin>000 00:00:00</depfailure-hrsmin>
    <depfailure-pct>0.00</depfailure-pct>
    <notprocessed-secs>84570</notprocessed-secs>
    <notprocessed-hrsmin>000 23:29:30</notprocessed-hrsmin>
    <notprocessed-pct>97.88</notprocessed-pct>
  </check>
  <check>
    ...
  </check>
</monitor>
```

Description of the Tags used in the above XML report document:

Tag	Description
<from-secs>	Begin time of report, in seconds after 01/01/1970
<from-date>	Begin time of report, in date format (i.e. mm/dd/yyyy)
<to-secs>	End time of report, in seconds after 01/01/1970
<to-date>	End time of report, in date format (i.e. mm/dd/yyyy)

<check/id>	ID of the Check, as it is used throughout the whole program
<check/displayname>	DisplayName of the Check, as it is used throughout the whole program
<check/success-secs>	Total amount of time (in seconds) that Check had status: Success
<check/success-hrsmin>	Total amount of time (in hh:mm format) that Check had status: Success
<check/success-pct>	Total amount of time (in percentage of total Report time) that Check had status: Success
<check/failure-secs>	Total amount of time (in seconds) that Check had status: Failure
<check/failure-hrsmin>	Total amount of time (in hh:mm format) that Check had status: Failure
<check/failure-pct>	Total amount of time (in percentage of total Report time) that Check had status: Failure
<check/uncertain-secs>	Total amount of time (in seconds) that Check had status: Uncertain
<check/uncertain-hrsmin>	Total amount of time (in hh:mm format) that Check had status: Uncertain
<check/uncertain-pct>	Total amount of time (in percentage of total Report time) that Check had status: Uncertain
<check/depfailure-secs>	Total amount of time (in seconds) that Check had status: Dependee Failure
<check/depfailure-hrsmin>	Total amount of time (in hh:mm format) that Check had status: Dependee Failure
<check/depfailure-pct>	Total amount of time (in percentage of total Report time) that Check had status: Dependee Failure
<check/maintenance-secs>	Total amount of time (in seconds) that Check had status: Maintenance
<check/maintenance-hrsmin>	Total amount of time (in hh:mm format) that Check had status: Maintenance
<check/maintenance-pct>	Total amount of time (in percentage of total Report time) that Check had status: Maintenance
<check/onhold-secs>	Total amount of time (in seconds) that Check had status: On Hold
<check/onhold-hrsmin>	Total amount of time (in hh:mm format) that Check had status: On Hold
<check/onhold-pct>	Total amount of time (in percentage of total Report time) that Check had status: On Hold
<check/notprocessed-secs>	Total amount of time (in seconds) that Check had status: Not Processed
<check/notprocessed-hrsmin>	Total amount of time (in hh:mm format) that Check had status: Not Processed
<check/notprocessed-pct>	Total amount of time (in percentage of total Report time) that Check had status: Not Processed

A.2. XML Detail Reports

To customize 'detail' reports, you need to make changes to the XSL file. Before you can make changes to the XSL file, a little understanding of the XML document is required.

The XML document is the result of the Report Creation Tool (either AXRGGUI.EXE or AXRGCMD.EXE). It has a reference to a static XSL document. This XSL document describes how the XML document should be displayed.

The XML document of a 'detail' report looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="stylesheets\DetailReport.xsl"?>
<monitor>
  <from-secs>1154124000</from-secs>
  <to-secs>1154210399</to-secs>
  <from-date>07/29/2006 12:00:00 AM</from-date>
```

```

<to-date>07/29/2006 11:59:59 PM</to-date>
<check>
  <id>10288</id>
  <displayname>www.monitortools.com - ICMP Ping</displayname>
  <checktype>ICMP</checktype>
  <checktype-id>10</checktype-id>
  <folder>\</folder>
  <event>
    <from-secs>1154124000</from-secs>
    <from-date>07/29/2006</from-date>
    <from-time>12:00:00 AM</from-time>
    <to-secs>1154202296</to-secs>
    <to-date>07/29/2006</to-date>
    <to-time>09:44:56 PM</to-time>
    <result-id>0</result-id>
    <result>Not monitored</result>
    <duration-secs>78296</duration-secs>
    <duration>000 21:44:56</duration>
    <reason>Not monitored</reason>
  </event>
  <event>
    ...
  </event>
</check>
<check>
  <id>10289</id>
  <displayname>flkjfskdlf - ICMP Ping</displayname>
  ...
  <event>
    ...
  </event>
  <event>
    ...
  </event>
</check>
</monitor>

```

Description of the Tags used in the above XML document:

Tag	Description
<from-secs>	Begin time of report, in seconds after 01/01/1970
<from-date>	Begin time of report, in date format (i.e. mm/dd/yyyy)
<to-secs>	End time of report, in seconds after 01/01/1970
<to-date>	End time of report, in date format (i.e. mm/dd/yyyy)
<check/id>	ID of the Check, as it is used throughout the whole program
<check/displayname>	DisplayName of the Check, as it is used throughout the whole program
<check/event/from-secs>	Begin time of the event, in seconds after 01/01/1970
<check/event/from-date>	Begin time of the event, in date format (i.e. mm/dd/yyyy)
<check/event/from-time>	Begin time of the event, in time format (i.e. hh:mm:ss)
<check/event/to-secs>	End time of the event, in seconds after 01/01/1970
<check/event/to-date>	End time of the event, in date format (i.e. mm/dd/yyyy)
<check/event/to-time>	End time of the event, in time format (i.e. hh:mm:ss)
<check/event/result>	The last Result of the Check, represented by a string
<check/event/result-id>	The last Result of the Check, described by a unique number. The Result ID's are described later in this chapter
<check/event/duration-secs>	Duration of the event, in seconds

<code><check/event/duration></code>	Duration of the event, formatted as: 'xx hrs yy min'
---	--

A.3. Contants

▼ Check Type ID

The `<checktype-id>` tag can hold any of the following pre-defined values:

Check Type ID	Description
0	<UNDEFINED TYPE>
1	<FOLDER>
10	ICMP
20	Disk Space
30	TCP/IP
31	POP3
32	SMTP
33	HTTP(s)
34	FTP
35	RSH
36	DNS
37	SNMP
38	NNTP
39	IMAP
40	NTP
41	Temperature
42	SNMP Trap Receive
43	SSH
50	Service
60	File
70	Anti-Virus / Anti-Spam
71	MS Active Directory
72	MS Hyper-V Server
73	MS Exchange
74	MS IIS Server
75	MS ISA Server
76	MS SharePoint Server
77	MS SQL Server
90	Event Log
100	VBScript
110	ODBC
111	Database (OLE DB)
112	Oracle
120	MS Terminal Server
130	CPU
140	Directory Size
150	Disk
160	Floppy
170	Memory

180	Printer
190	Process
200	Humidity
201	Power
202	Light
203	Motion
204	Smoke
205	Door
206	Resistance
207	Switch (NC)
208	Switch (NO)
210	Wetness
220	Shceduled Task
240	SMTP to POP3
250	MSMQ
260	Serial Device
270	TFTP
280	Remote Command
290	PowerShell
300	Radius
310	SFTP

▼ Result ID

The `<result-id>` tag can hold any of the following pre-defined values:

Result ID	Description
0	Uncertain
1	Success
2	Error
3	Failure
4	Maintenance
5	On Hold
6	Dependee Error
7	Dependee Failure
99	Not Processed

APPENDIX B: Web Interface XML Tags

To customize 'availability' reports, you need to make changes to the XSL file. Before you can make changes to the XSL file, a little understanding of the XML document is required.

XML data is represented as a series of XML Tags. Each set of Tags (record) can be used as an interface to a database. For instance, you can import the XML data in a MS SQL database regularly.

As mentioned before, XML allows custom tags and a custom document structure; ActiveXperts Network Monitor defines its own tags for its Web Views.

Each Monitoring Check is enclosed by `<check>` and `</check>` tags, and describes the last result of the check as processed by the Network Monitor Engine. The following tags are used to describe the result of the check:

Tag	Description
<code><id></code>	Unique ID of the Check; The ID is a long integer, and is also the key in the database (CONFIG.MDB) for the check
<code><displayname></code>	DisplayName of the Check, as it is used throughout the whole program
<code><folder></code>	Full Folder Path where Check is located
<code><type-id></code>	Type of Check, also called 'Check'. Every Check has a Unique ID (for instance: ICMP=10, DiskSpace=20, Service=50, etc.). Type ID's are described later in this chapter
<code><type></code>	Type of Check
<code><result-id></code>	The last Result of the Check, described by a unique number. The Result ID's are described later in this chapter
<code><result></code>	The Last Result of the Check, shown as a string
<code><data></code>	The actual data (if exists) of the monitored item.
<code><bitmap></code>	Bitmap indicating the result of the processed Check
<code><explanation></code>	Basic explanation of the result
<code><comments></code>	Additional comments to the result
<code><update-secs></code>	Last Update time, in seconds after 01/01/1970
<code><update></code>	Last Update time, shown as a friendly string

APPENDIX C: Notification Variables

Notification Variables are variables which are substituted by the Network Monitor Engine when an action is triggered or a notification is sent.

There are several places in the Network Monitor software where you can use System Variables. You can use system variables inside Message Templates, on the command prompt when running an executable or VBScript program, and in SNMP Trap notifications.

Notification Variables must be enclosed between `<%` and `%>` tags, for example: `<% DATE %>..`

The following variables can be used:

- ◆ `<%DATE%>` – The Date of the event;
- ◆ `<%TIME%>` – The Time of the event;
- ◆ `<%ID%>` – The unique ID of the Monitoring Check;
- ◆ `<%DISPLAYNAME%>` – Name of the Monitoring Check;
- ◆ `<%TYPE-ID%>` – Type of check. Each check has a unique ID;
- ◆ `<%TYPE%>` – Type of check (friendly string);
- ◆ `<%SERVER%>` – Name of the server/device that is being checked;
- ◆ `<%RESULT-ID%>` – The Result ID of the event. Each Result has a unique ID;
- ◆ `<%RESULT%>` – The Result of the event (friendly string);
- ◆ `<%DATA%>` – Actual data item;
- ◆ `<%EXPLANATION%>` – Detailed description of the result of the event.

▼ DATE variable

The date the event occurred.

▼ TIME variable

The time the event occurred.

▼ ID variable

The unique ID of the Monitoring Check. Each check has a unique ID.

▼ DISPLAYNAME variable

The description of the Monitoring Check. Operators can change the display name by changing the Display Name field in the General Settings of the properties of that check.

▼ TYPE-ID variable

Type of check. Each check has a unique ID. Appendix A.3. contains an overview of all Check Type ID's and the corresponding descriptions.

▼ TYPE variable

Type of check (friendly string).

▼ SERVER variable

The server/device that was checked. In most cases, the SERVER name will be a hostname, NetBIOS name or an IP number. It depends on the kind of check that is being performed.

▼ RESULT-ID variable

The Result ID of the Event. Each Result has a unique ID. Appendix A.3. contains an overview of all Result ID's.

▼ RESULT variable

The Result of the Event (friendly string).

▼ DATA variable

Actual data item (if available). The variable holds the value that is retrieved. For instance, when monitoring CPU usage, the 'Data' variable holds the actual CPU usage, for instance: 60.

▼ EXPLANATION variable

Additional information about the result of the last check.