## Contents

### Introduction
- Introduction to GFI Network Server Monitor .......................................................... 1
- Key features............................................................................................................... 1
- GFI Network Server Monitor components ............................................................ 3
  - Network Monitor Engine ..................................................................................... 4
  - Network Monitor Manager application ............................................................... 4
- License Scheme ...................................................................................................... 4

### Installing GFI Network Server Monitor
- System Requirements ............................................................................................... 5
- Installation Procedure ............................................................................................... 5
- GFI Network Server Monitor Quick Configuration Wizard ..................................... 7
- Entering your License key after installation ............................................................. 9

### Configuring GFI Network Server Monitor
- Getting started with GFI Network Server Monitor .................................................. 11
- Creating Monitor Rules ........................................................................................... 12
  - Selecting what to monitor .................................................................................... 13
  - Configure the notifications to be sent ................................................................. 14
  - Configure action (if any) to be taken .................................................................. 16
  - Run a program after an alert is triggered ......................................................... 16
  - Advanced options ............................................................................................... 18
  - Viewing status of the rule. .................................................................................... 19
- Creating folders to organize rules .......................................................................... 20

### Configuring monitor functions
- Introduction ................................................................................................................. 23
- CPU Usage .................................................................................................................. 23
- Directory Size ............................................................................................................ 24
- Disk Drive ................................................................................................................... 24
- Disk Space .................................................................................................................. 25
- DNS Server ............................................................................................................... 26
- Event Log .................................................................................................................... 26
- Exchange 2000/2003 ............................................................................................... 28
- ISA server 2000 ....................................................................................................... 28
- File Existence .......................................................................................................... 29
- File Size ...................................................................................................................... 30
- FTP ............................................................................................................................... 31
- HTTP/HTTPs ............................................................................................................ 32
- ICMP/Ping ............................................................................................................... 33
- IMAP Mail Server availability .................................................................................. 34
- MS SQL / ADO Database ......................................................................................... 35
- Novell NDS ................................................................................................................ 35
- NNTP News Server availability ............................................................................. 36
- NTP Time Server availability .................................................................................. 37
- ODBC Database ....................................................................................................... 37
- Oracle Database ....................................................................................................... 39
- POP3 Mail Server availability .................................................................................. 40
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printer Availability</td>
<td>40</td>
</tr>
<tr>
<td>Process</td>
<td>42</td>
</tr>
<tr>
<td>Service</td>
<td>43</td>
</tr>
<tr>
<td>SMTP Mail Server availability</td>
<td>44</td>
</tr>
<tr>
<td>SNMP function</td>
<td>45</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>46</td>
</tr>
<tr>
<td>UNIX RSH Shell Script</td>
<td>47</td>
</tr>
<tr>
<td>Users &amp; Groups</td>
<td>48</td>
</tr>
<tr>
<td>VBScript monitor function</td>
<td>48</td>
</tr>
<tr>
<td><strong>Advanced features</strong></td>
<td></td>
</tr>
<tr>
<td>Configuring Logging</td>
<td>81</td>
</tr>
<tr>
<td>Configuring dependencies</td>
<td>81</td>
</tr>
<tr>
<td>Configuring Global Maintenance Periods</td>
<td>82</td>
</tr>
<tr>
<td>Setting Default Rule Options</td>
<td>84</td>
</tr>
<tr>
<td>Monitoring defaults</td>
<td>84</td>
</tr>
<tr>
<td>Notification defaults</td>
<td>84</td>
</tr>
<tr>
<td>Import, Export and Clear configuration settings</td>
<td>85</td>
</tr>
<tr>
<td>Import configuration settings</td>
<td>85</td>
</tr>
<tr>
<td>Export configuration settings</td>
<td>86</td>
</tr>
<tr>
<td>Clear configuration settings</td>
<td>87</td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td></td>
</tr>
<tr>
<td>Introduction to reporting</td>
<td>73</td>
</tr>
<tr>
<td>Detailed Availability Report</td>
<td>73</td>
</tr>
<tr>
<td>Summary Availability Report</td>
<td>75</td>
</tr>
<tr>
<td><strong>Writing your own monitoring functions</strong></td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>77</td>
</tr>
<tr>
<td>Writing a script/function</td>
<td>77</td>
</tr>
<tr>
<td>Adding a monitor function written in VBScript</td>
<td>78</td>
</tr>
<tr>
<td>WMI (Windows Management Instrumentation)</td>
<td>79</td>
</tr>
<tr>
<td>ADSI (Active Directory Service Interfaces)</td>
<td>80</td>
</tr>
<tr>
<td><strong>Remote web monitor</strong></td>
<td></td>
</tr>
<tr>
<td>Introduction to the remote web monitor</td>
<td>63</td>
</tr>
<tr>
<td>Normal web monitoring page</td>
<td>63</td>
</tr>
<tr>
<td>Mobile/handheld device monitoring page</td>
<td>64</td>
</tr>
<tr>
<td>Configuring the remote web monitor</td>
<td>65</td>
</tr>
<tr>
<td>Using the internal web server</td>
<td>66</td>
</tr>
<tr>
<td>Configuring IIS as the web server</td>
<td>66</td>
</tr>
<tr>
<td>Securing as the web server</td>
<td>69</td>
</tr>
<tr>
<td><strong>Message Templates</strong></td>
<td></td>
</tr>
<tr>
<td>Message Template Example</td>
<td>61</td>
</tr>
<tr>
<td><strong>SMS Notifications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Network Notifications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>E-mail Notifications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Remote web monitor</strong></td>
<td></td>
</tr>
<tr>
<td>Introduction to the remote web monitor</td>
<td>63</td>
</tr>
<tr>
<td>Normal web monitoring page</td>
<td>63</td>
</tr>
<tr>
<td>Mobile/handheld device monitoring page</td>
<td>64</td>
</tr>
<tr>
<td>Configuring the remote web monitor</td>
<td>65</td>
</tr>
<tr>
<td>Using the internal web server</td>
<td>66</td>
</tr>
<tr>
<td>Configuring IIS as the web server</td>
<td>66</td>
</tr>
<tr>
<td>Securing as the web server</td>
<td>69</td>
</tr>
<tr>
<td><strong>Message Templates</strong></td>
<td></td>
</tr>
<tr>
<td>Message Template Example</td>
<td>61</td>
</tr>
<tr>
<td><strong>SMS Notifications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Network Notifications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>E-mail Notifications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Remote web monitor</strong></td>
<td></td>
</tr>
<tr>
<td>Introduction to the remote web monitor</td>
<td>63</td>
</tr>
<tr>
<td>Normal web monitoring page</td>
<td>63</td>
</tr>
<tr>
<td>Mobile/handheld device monitoring page</td>
<td>64</td>
</tr>
<tr>
<td>Configuring the remote web monitor</td>
<td>65</td>
</tr>
<tr>
<td>Using the internal web server</td>
<td>66</td>
</tr>
<tr>
<td>Configuring IIS as the web server</td>
<td>66</td>
</tr>
<tr>
<td>Securing as the web server</td>
<td>69</td>
</tr>
<tr>
<td><strong>Message Templates</strong></td>
<td></td>
</tr>
<tr>
<td>Message Template Example</td>
<td>61</td>
</tr>
<tr>
<td><strong>SMS Notifications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Network Notifications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>E-mail Notifications</strong></td>
<td></td>
</tr>
</tbody>
</table>
Renaming computers .................................................................................................. 87

**Troubleshooting** 89
  Introduction ............................................................................................................. 89
  Knowledgebase ........................................................................................................ 89
  Request support via e-mail ..................................................................................... 89
  Request support via web chat .................................................................................. 90
  Request support via phone ...................................................................................... 90
  Web Forum ............................................................................................................... 90
  Build notifications .................................................................................................. 90

**Index** 91
Introduction

Introduction to GFI Network Server Monitor

GFI Network Server Monitor is a network & server monitoring tool that allows administrators to monitor the network for failures or irregularities automatically. With GFI Network Server Monitor, you can identify issues and fix unexpected conditions before your users (or managers) report them to you!

GFI Network Server Monitor maximizes network availability by monitoring all aspects of your servers (including UNIX/LINUX servers), workstations and devices (routers, etc.). When it detects a failure, GFI Network Server Monitor can alert you by email, pager or SMS, as well as taking corrective action by, for example, rebooting the machine, restarting the service or running a script.

GFI Network Server Monitor is easy to set up and use, and is competitively priced. You can set any amount of rules and customize each rule to suit your needs and network set-up.

Key features

**Enterprise class architecture**

GFI Network Server Monitor consists of a monitoring service (called the Network Monitor Engine) and a separate management interface (the Network Manager). No agent software needs to be installed on the machines you wish to monitor. The Network Monitor Engine is multi-threading and can run 16 checks at a time. This software architecture allows for high reliability and scalability to monitor both large and small networks.

**In built Exchange 2000/2003 monitoring**

Out of the box, GFI Network Server Monitor monitors the status of your Exchange Server by monitoring critical Exchange services and performance counters (Information Store, mailboxes, SMTP service, etc.).

**Monitor your database servers (SQL/ORACLE/ODBC)**

GFI Network Server Monitor can check the availability of all leading database applications. Out of the box, it can monitor Microsoft SQL server via ADO and Oracle via SQL*Net. Oracle servers can be monitored by a TNS ping check and by a logon/logoff. Other databases such as Access, FoxPro, Paradox, SyBase, Informix, IBM DB2 and many more can be monitored via ODBC.

**Monitor remote Event Logs**

GFI Network Server Monitor can scan Windows Event logs on local or remote computers and look for specific Event Sources, Categories,
and Event ID’s and for patterns in the Description of the Event. In addition it can look for multiple events occurring in a specific time interval, for example a Mcafee or Norton virus alert posted in the last 30 minutes.

**Built-in computer monitor functions**

- CPU usage function – Ensure that a processor’s usage does not go beyond a certain level
- Directory size function – Ensure that a particular directory (for example, a user’s home directory) does not take up more than x amount of drive space
- Disk drive function - Monitor the physical status of the disk
- Disk space function – Check if sufficient disk space is available
- File existence function – Monitor the existence of a particular file; e.g. results of scheduled batch jobs
- File size function – Monitor the size of particular files, for example, critical log files.

**Built in Internet Service functions**

- HTTP function – Check availability of HTTP and Https sites. Pass credentials if required.
- Website content checking – Check website content by specifying a text pattern to check for
- FTP function – check availability of an FTP server/site.
- ICMP ping function - Checks a remote host for availability
- DNS server function - Check if DNS server by reading an 'A' record and verifying the result
- SMTP server function - Checks mail server by establishing a connection and doing a handshake to verify SMTP protocol is working correctly
- POP3 server function - Checks POP3 servers by establishing a connection and doing a handshake
- NNTP news server function - Checks connection and does a handshake
- SNMP function – Monitor specific variables on remote machines or devices via the SNMP GET message.
- TCP port function – Checks if a port is responding and check its response
- UDP function – Monitor UDP ports
- NTP function – Monitor timeservers

**Alert notification via email, pager or SMS**

When it detects a failure, GFI Network Server Monitor can send alerts via SMS, pager, email or a network message. SMS messages are sent through either an SMS service provider (SMSC), or directly through a connected GSM phone/modem. All notifications can be customized using variables. Recipients can be configured globally for all rules.

**Take corrective action automatically**
After an unexpected condition has occurred, GFI Network Server Monitor can automatically correct the problem by restarting a service (or multiple services) upon failure; rebooting a server upon failure; or launching an executable, batch job or VBScript.

**Monitor Windows servers & workstations, UNIX/Linux & Novell**

GFI Network Server Monitor can monitor multiple platforms simultaneously including UNIX/Linux and Novell. UNIX/Linux servers can be monitored by checking the output of RSH scripts.

**Monitor processes and services & CPU usage**

GFI Network Server Monitor enables you to check critical processes and services on local and remote computers. You can also monitor the CPU usage of a machine. This way, you can ensure that virtually any application is running properly.

**Custom monitor monitoring using VBscript & RSH**

Although GFI Network Server Monitor includes an extensive set of default monitoring functions, you can build your own custom checks by writing a VBscript (Windows) or a RSH shell script (UNIX). From VBscript, you can use make use of WMI and ADSI. WMI is an interface to a broad range of hardware/software/OS-related properties of a computer, allowing you to perform almost any check. Using ADSI you can interface to Active Directory. GFI Network Server Monitor includes a library of sample scripts, and others are continuously added to the website.

**Monitor users, groups & other Active Directory information**

Use GFI Network Server Monitor to monitor directory information. For example, monitor group membership of the domain admins group. You can also check user accounts (locked out, disabled, etc.), computer accounts, groups, group membership, Organizational units, and so on. A subset of NTDS (NT4-based SAM account database), and Novell NDS Directory Service can be queried too.

**Reporting**

GFI Network Server Monitor allows you to create reports that detail the availability of your network resources. Create reports directly in HTML, or generate XML/CSV reports, which you can export to your favorite application.

Other features

- Configure maintenance periods to avoid alerts being sent during scheduled maintenance
- Advanced logging options to text file or event log
- Configure dependencies to avoid multiple alerts for error conditions dependent on each other
- Read-only mode for users who are not allowed to make changes to the configuration

**GFI Network Server Monitor components**

The architecture of the GFI Network Server Monitor is client/server based: a central monitoring service runs on a Windows NT or higher computer; it monitors servers and workstations in your LAN, WAN or
even outside your enterprise. No additional software is required on the monitored servers.

**Network Monitor Engine**

The GFI Network Server Monitor Engine is a Windows Service (GFINMSVC.EXE), and is the actual monitoring program. It polls the servers in your LAN/WAN for availability at specific time intervals. This service is multithreading, allowing the service to monitor many servers simultaneously. The service is responsible for notification, actions, recovery, logging, and so on.

**NOTE:** GFI Network Server 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 the job.

**Network Monitor Manager application**

The GFI Network Server Monitor Manager application (GFINMAPP.EXE) is used to view the results, and to make changes to the configuration. This manager program allows you to visually monitor the network, and to make changes to the program configuration. You can install the Manager application on any workstation/server in your LAN/WAN.

The Manager application makes a connection to the central GFI Network Server Monitor service, to write configuration information, and to read monitoring information.

The Manager application can be installed on any Windows 98, Windows NT or higher computer (workstation or server).

**License Scheme**

The GFI Network Server Monitor software has the following licensing scheme:

**5 Server License** - This license allows you to monitor up to 5 servers/workstations on your network.

**15 Server License** - This license allows you to monitor up to 15 servers/workstations on your network.

**Unlimited server license** - This license allows you to monitor an unlimited number of servers/workstations on your network.
Installing GFI Network Server Monitor

System Requirements

The Machine on which you will be installing GFI Network Server Monitor requires the following:

- Windows 2000 (SP1 or higher), 2003 or XP Pro
- Windows scripting host 5.5 or higher (Included in Internet Explorer 6 and in Service pack 2 of Internet Explorer 5.5). You can download it separately from www.microsoft.com/scripting.

Any machines that you wish to monitor:

- If you are monitoring a Windows NT 4 machine, and are using scripts that use WMI, you need to install WMI on that machine. (See above for link)
- If you are monitoring a machine and running a function that uses VBscript, you need to ensure that the host you are monitoring has Windows Scripting Host 5.5 or higher installed. (See above for link)

Installation Procedure

The installation will install the actual monitor service, the Manager application and the setup files for additional Manager applications on other computers.

Before you run the installation procedure please make sure that:

1. You are logged on as Administrator.
2. Run GFI Network Server Monitor set-up by double-clicking on the file gfinsm.exe. The set-up file will be uncompressed, after which the setup wizard will start. Click Next to start installation.
3. In the License agreement dialog box, click Yes to accept the agreement and continue the installation.
4. Enter your company name, fax number and License key. If you are evaluating the product, leave the default 'Evaluation' key. Click Next. 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 License key. If you are installing the software in evaluation mode, a confirmation message will appear.

5. Choose Destination Folder - Setup will copy the service, the Manager application, the Manager Setup files and other components to this location. Please be sure to have at least 10 megabytes available, depending on the type of installation.
6. Specify service Account: The GFI Network Server Monitor service must run with administrator credentials. It is recommended to provide a Domain Admin or Enterprise Admin account, because most probably, GFI Network Server Monitor will need administrative rights to access the servers in the domain. However, it’s not mandatory to provide a Domain/Enterprise Admin account; for every monitoring rule, separate credentials can be provided.

7. Set-up will confirm installation and will copy all program files to the selected destination, and finish the installation by creating a GFI Network Server Monitor program group. Click **Finish** to finish setup.

---

**GFI Network Server Monitor Quick Configuration Wizard**

After you complete setup, or the first time you start the GFI Network Server Monitor Manager application, the Quick Configuration Wizard starts up, which guides you through a number of basic configuration steps:
1. In the first step, enter your mail server name or ip, as well as your e-mail address. This address will be used to send the alerts to.

2. In the second step, enter your network user name. This will be used to send you network popup notifications if required.
3. In the third step you can configure the default monitor interval, as well as the default number of failures before a rule will issue an alert.
4. Step 4 asks you if you want to add a number of sample rules to the configuration.
   After this, click finish to end the ‘Quick configuration wizard’

**Entering your License key after installation**

If you have purchased GFI Network Server Monitor, you can enter your License key by going to ‘Licensing’ in the tools menu and entering your License key.

If you are evaluating GFI Network Server Monitor, it will time out after 60 days (with evaluation key). If you then decide to purchase GFI Network Server Monitor, you can just enter the License key here without having to re-install.

You must license GFI Network Server Monitor for the number of servers that you wish to monitor.

Entering the License key should not be confused with the process of registering your company details on our website. This is important, since it allows us to give you support and notify you of important product news. Register on:

http://www.gfi.com/pages/regfrm.htm
Getting started with GFI Network Server Monitor

After you have installed GFI Network Server Monitor, you need to decide what you want to monitor. For example, you may wish to monitor that your http server is up and that it is serving the content that you put there. For each thing that you want to monitor, you must create a monitor rule. A monitor rule performs a particular check. You can specify different actions, alerts etc. for each monitor function. The following monitor functions are included by default in GFI Network Server Monitor:

- CPU Usage – monitors CPU Usage of one or more processor(s).
- Directory Size – monitor directories, like user’s Home Directories, or common Department Folders;
- Disk Drive – monitors physical disk drives;
- Disk Space – checks disk space
- DNS Server – checks if the DNS server if functioning well;
- Event Logs – checks for certain types of events and their content;
- Exchange Server – monitors the status of the Exchange services and the most important performance counters;
- ISA Server – monitors the status of the ISA services;
- File Existence – checks if files exists and its contents;
- File Size – monitor file sizes;
- HTTP/HTTPS availability – checks availability and content of websites;
- ICMP/Ping availability – checks if workstations/servers are listening for incoming ICMP packets;
- MS SQL / ADO Database – check availability of Microsoft SQL databases.
- NNTP News Server – checks availability of News Servers;
- NTP Time Server – checks status of Time Server;
- ODBC Databases – checks availability of ODBC compatible databases.
- Oracle Databases – checks for availability of Oracle database by using the SQLNet interface;
- POP3 mail servers – checks availability of PO3 mail servers;
- Printers – checks status of printers;
• Processes – checks processes on local- and remote computers;
• Services – checks status of services;
• SMTP availability – checks availability of SMTP mail servers;
• SNMP availability – query a computer or device using the SNMP ("Simple Network Management Protocol") protocol, and analyze the result;
• TCP/IP connectivity – checks if a connection can be made on specific TCP ports;
• UDP ports – monitors UDP ports by sending an echo request;
• UNIX RSH Shell Script – checks UNIX/LINUX servers by executing remote shell scripts;
• User/groups – checks groups and group membership;

You can add further monitor functions by writing them in VBScript. You can leverage WMI and ADSI in these scripts.

A more detailed description of the monitor functions can be found in the chapter ‘Configuring Monitor Functions’

Creating Monitor Rules

Screenshot 6 - Network Server Monitor Manager

After you have decided what you want to monitor, you have to create monitor rules in the GFI Network Server Monitor Manager. The GFI Network Server Monitor Manager application is divided into three views:

• Folder view (left view) – graphical representation of the folders;
• Server view (right view) – list of rules in that folder.
• Activity Log view (bottom view) – shows the activity of the GFI Network Server Monitor service.

To add a new Monitor Rule:
1. Startup the GFI Network Server Monitor Manager from the GFI Network Server Monitor program group.
2. On the File menu, click New and choose Monitor Rule; Alternatively click New Monitor Rule on the toolbar.
3. Now, the Rule Properties dialog pops up. This dialog contains 5 tabs:
   - ‘Monitor What’;
   - Notifications (Mail/Network) – E-mail and NetBIOS notifications;
   - Notifications (Pager) – Pager notifications;
   - Actions (Programs) – Run batch file, exe-file or VBScript programs;
   - Actions (Reboot/Restart) – Restart service(s) or reboot server.

Selecting what to monitor

4. In the ‘Monitor What’ tab, select the check you wish to perform from the Monitor Function drop-down box; a ‘Monitor Rule properties’ dialog will popup; In the next chapter, specific Monitor functions are described in more detail;

5. In the Display Name box, edit the custom display name; this name will also be used in the log files and reports;

6. In the Monitor every field, specify how often a Monitor Function will be executed. By default, a Monitor Rule will be executed every 120 seconds. This default can be changed from the Options dialog in the Tools Menu.

7. In the Consider Failure After field, specify the number of consecutive errors that must occur before a Monitor Rule will be considered as Failed; by default, a Monitor Rule will be considered as Failed after 3 consecutive errors, i.e. when the Monitor Function fails 3 times in a row.
Configure the notifications to be sent

8. Now select the Notifications (Mail/Network) tab, and configure the following fields:
   - Notify when server/device goes offline — If server/device goes offline, send an e-mail/network notification to the operators. These operators can either be extracted from the global defined recipient list, or from a custom recipient list that is used for this event only;
   - Notify when server/device goes online — If server/device turns from offline to online, send an e-mail/network notification to the operators as described above;
9. If you want an alert to be sent via SMS or Pager, select the Notifications (SMS/Pager) tab, and configure the following fields:

- Notify when server/device goes offline – If server goes offline, send an SMS/Pager message to the operators. Fill in the number to be dialed; Note that the global pager dialing rules are used to dial the actual number.
- Notify when server/device goes online – If server turns from offline to online, send an SMS/Pager message to the operators. Fill in the number to be dialed.
Configure action (if any) to be taken

10. Now select the Actions (Reboot/Restart) tab. You can define several actions for each individual monitor rule. Actions are taken when a server fails, or when a server recovers from a failure. There are no general settings for Actions; all settings are made in the properties of the monitor rule. You can configure the following 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 might be a good idea to restart the W3SVC 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 in order to recover from a failure.

- **Run Program** - You can run a program after a failure has occurred. GFI Network Server Monitor supports three different types of programs: Executable files; Batch programs and VBScript programs.

Run a program after an alert is triggered

You can pass parameters to these programs on the command line. You can also use system variables as parameters, like `<% DISPLAYNAME %>` and `<% SERVER %>`. Variables are substituted when the program or script is launched. The system variables are the same ones as described in the Message Templates section.
There are three sample programs included: SAMPLE.BAT, SAMPLE.EXE, and SAMPLE.VBS. These samples all write a line of text to a file called <INSTALL-DIR>\SERVER\TMP\SAMPLES.LOG.

If you want to run a program after an alert triggers, select the Actions (Program) tab, and configure the following fields:

- Run this program (.exe or .bat) when server/device goes offline
- Run this program (.exe or .bat) when server/device goes online
- Run this program (.vbs) when server/device goes offline
- Run this program (.vbs) when server/device goes online.
For each rule you can also set advanced options:

**Notification frequency:** Allows you to limit the number of notifications that GFI Network Server Monitor sends.

**Action frequency:** Allows you to limit the number of times that GFI Network Server Monitor will perform an action.

**Server maintenance periods:** This option allows you to configure ‘Maintenance periods’, which are time intervals during which the rule will not perform the check. For example, during backup hours, some services/daemons will be stopped to avoid open files, Mail Servers will be stopped, and so on. To avoid notifications during this time you can define ‘Maintenance Periods’. During these hours, no actions will be taken or alerts sent in case of a failure. To configure

1. Click on ‘Configure Maintenance periods’
2. Choose either Never, Only Once or Day of Week.
‘Only Once’ - provide start date and time, and number of hours the computer and devices will be unavailable;

‘Day of Week’, provide the days of the week that the computers and devices will be unavailable as well as start time and number of hours the servers will be unavailable.

Note: Maintenance periods can be configured globally (for all monitor rules) from the Tools > Options > Maintenance Periods tab. The global Maintenance periods are then inherited by all Monitor Rules. This is required by many system operators. Let’s say a company has maintenance on every Friday at 11:00 pm for nearly all servers (use the Global maintenance Periods for that). But for one server (server ‘A’), maintenance is done on Saturday at 09:00 am. Configure individual Maintenance Periods for this server ‘A’.

Dependencies – The dependencies function allows you to configure servers/functions that are dependent on each other. This prevents a flood of messages when for example your internet connection goes down. To check what dependencies this rule has, click on the ‘Show dependencies’ button.

The actual dependencies are configured by going to the Tools menu and selecting Dependencies.

Viewing status of the rule.

Now click OK to create the rule. The rule will show up in the right hand pane of the GFI Network Server Monitor manager. To test out the rule, you can select ‘Monitor Server Now’ from the Action menu. In the bottom pane, the GFI Network Server Monitor manager will show what is happening. The rule status will then change depending on the outcome of the check.

Here is a list of all possible state values (with corresponding icons) and their meanings:
OK – The Rule meets all the conditions. The corresponding server/device/application is working fine.

Error – When a Rule doesn’t meet the monitor function condition once, it’s considered as an Error. For example if you have setup a http monitor function, and the web server that you are monitoring does not respond, the rule is in error until it does not respond 3 times in a row (depending on what you configured). This is handy because if a check fails once, for example because a router on the internet has a hick-up, you don’t want to receive an alert, because the problem has nothing to do with the actual server. So, the Rule is in the Error state. But when this error happens a couple a times in a row, it’s considered as a Failure.

Failure – A Failure is the occurrence of 1 or more Errors in a row. You can configure what number of errors constitutes a failure. Only when the error happens x times in a row, it’s a considered a Failure. Only then, notifications are sent out and actions are taken.

For instance, when you configure a Rule based on the ‘ICMP Ping’ function, you should configure to the rule to fail only after a number of errors in a row, for example 5. Only then will the state of the Rule change to ‘Failure’.

Maintenance – When the result of a rule is not successful during Maintenance hours, it won't be considered as an ordinary Error or a Failure. The rule state will be shown as ‘Maintenance’. No notifications will be sent and no actions will be triggered.

Failure by Dependee – When a monitor function rule fails (after a number of errors in a row) as a result of another failed check, and there is a dependency configured between them, the rule status will be shown as ‘Failure by dependee’. 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 rules for both ‘S1’ and ‘R’. You should make ‘S1’ dependent of ‘R’. In that case, if ‘R’ fails, you won’t get actions/notifications from ‘S1’.

On Hold – You can put a Rule ‘On Hold’, so it won’t be processed by the Network Monitor Engine.

Not Monitored – When a Rule cannot be processed by the Engine, the state is set to Not Monitored. This happens if the Network Server Monitor service is stopped. Alternatively if a rule requires for example the SNMP service to be installed, but this service is not installed on the machine running the Network Server Monitor service, then the rule will be shown as 'Not Monitored'.

Uncertain – When the result of the Rule cannot be determined by the Engine, the state is set to Uncertain. For example, if the server on which a monitor function checks Disc Space can no longer be accessed, then the rule status is set to ‘Uncertain’. Because the Network Monitor Engine cannot determine the Disk Space any longer.

Creating folders to organize rules

GFI Network Server Monitor Manager allows you to make folders under the root folder, so that you can organize your rule sets better. To add a new folder:
1. On the File menu, click New and choose Folder;
2. In the Name field, type the name of the new folder.
3. Alternatively you can use the New Folder button on the toolbar.

**To edit the name of a folder:**
1. Select the Folder you want to edit;
2. Choose Properties from the File menu;
3. Type a New Name for the Folder.

**To delete a folder:**
1. Select the Folder you want to delete;
2. Choose Delete from the File menu;
Configuring monitor functions

Introduction
As soon as you add a new Monitor Rule, you must select the Monitor Function. GFI Network Server Monitor supports a wide range of built-in Monitor Functions. In this chapter, each monitor function is explained in more detail and how you should configure each monitor function.

CPU Usage
Note: This monitor function requires WMI to be installed on the computer running the GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript, which uses WMI, with the parameters you specify in the monitor function setup screen. WMI is only available on Windows 2000 and higher machines, so this monitor function can only be used if both the GFI Network Server Monitor machine and the machine to be monitored are running Windows 2000 or higher.

GFI Network Server Monitor provides the ‘CPU Usage’ function to monitor processor(s) on Windows platforms. Whenever the CPU load exceeds the limit, a notification is generated or an action can be triggered.

A CPU Usage function takes the following parameters:
- Server – The NetBIOS name, DNS name or the IP address of the server you want to monitor;
- Max. CPU Usage – Maximum allowed CPU usage (%).
Directory Size

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. You can use this function to implement an effective, but low cost disk quota system.

A Directory Size function takes the following parameters:

- Directory – the directory in UNC (‘Universal Naming Convention’) format. For instance: \server01\public\docs;
- Used space limit – maximum number of KB allowed in the directory.

Disk Drive

Note: This monitor function requires WMI to be installed on the computer running the GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript, which uses WMI, with the parameters you specify in the monitor function setup screen. WMI is only available on Windows 2000 and higher machines, so this monitor function can only be used if both the GFI Network Server Monitor machine and the machine to be monitored are running Windows 2000 or higher.
GFI Network Server Monitor can monitor the physical health disk drives on servers and workstations running Windows.

A Disk Drive function takes the following parameters:

- **Server** – The NetBIOS name, DNS name or the IP address of the server you want to monitor;

---

### Disk Space

![Screenshot 17 - Disk space monitor function properties](image_url)

GFI Network Server Monitor can check for free disk space on local and remote computers. This can be handy to proactively avoid server or workstation down time. It can also notify you if used space gets too high.

A Disk Space function takes the following parameters:

- **Server** – the NetBIOS name, DNS name or the IP address of the server/workstation you want to monitor;
- **Drive** – the Drive letter as it appears on the remote server;
- **Free space / Used space** – In case of ‘Free space’, the server is checked for a minimum available space specified by the number of MB’s that you enter. In case of ‘Used space’, the server is checked for a maximum used space specified by the number of MB’s that you enter.
- **MB** – the upper/lower limit in Megabytes;
- **Log on with same account / Log on with other account** – Choose the account to be used by the GFI Network Server Monitor service to check the remote server. By default, the service account of the GFI Network Server Monitor service is used.
DNS Server

GFI Network Server Monitor can read an ‘A record’ on a DNS server and verify if this ‘A record’ includes the expected associated IP address.

A DNS Server function takes the following parameters:

- **DNS Server** – the IP address or hostname of the DNS server that you want to check;
- **‘A record’** – an A record that must be defined on the DNS Server. This can be an A record of a primary or secondary zone;
- **IP address** – the expected IP number. If the query result does not include the given IP address, the function will fail. Otherwise, the function will succeed.

**NOTE:** A DNS query can return more than one IP address.

Event Log

Note: This monitor function requires WMI to be installed on the computer running the GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript, which uses WMI, with the parameters you specify in the monitor function setup screen. WMI is only available on Windows 2000 and higher machines, so this monitor function can only be used if both the GFI Network Server Monitor machine and the machine to be monitored are running Windows 2000 or higher.
GFI Network Server 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 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 might 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.

An Event Log function takes the following parameters:

- **Server** – The NetBIOS name, DNS name or the IP address of the server 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.);
- **Log on with same account / Log on with other account** – Choose the account to be used by the GFI Network Server Monitor service to check the remote server. By default, the service account of the GFI Network Server Monitor service is used;
- **Consider as Error if Event does (NOT) exist** – If all conditions are met for the Event Log entry, will the situation be considered as an error or as a success?
- **Information/Warning/...** – Filter these event types;
- **Event Source** – Filter events that match this Event Source;
• Category – Filter events that match this Event Category;
• Event ID – Filter events that match this Event ID;
• User – Filter events that match this User;
• Only Events from the last x minutes – This option allows you to discard errors that happened in the past. Use this option, if you don’t want to be notified about error events that happened in the past (for example a week ago).
• Description matches string – Filter events that match the description string in the Event Message.

Exchange 2000/2003

Note: This monitor function requires WMI to be installed on the computer running the GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript, which uses WMI, with the parameters you specify in the monitor function setup screen.

GFI Network Server Monitor monitors the status of the Exchange services, and the most important performance counters. Among these performance counters are: performance counters of the Information Store, performance counters of Mailboxes, performance counters of Public Folders, and performance counters of the SMTP service. If it drops too low you’re immediately notified.

If you want, you can extend the Exchange check function by checking more services and monitoring more performance counters.

An Exchange 2000 function takes the following parameters:
• Server – The NetBIOS name, DNS name or the IP address of the Exchange server you want to monitor
• Exchange version – Indicate the Exchange server version you are monitoring

ISA server 2000

Note: This monitor function requires WMI to be installed on the computer running the GFI Network Server Monitor as well as on the
computer being monitored. The monitor function will create a VBscript, which uses WMI, with the parameters you specify in the monitor function setup screen.

Screenshot 21 - ISA server monitor function properties

GFI Network Server Monitor monitors the status of the ISA server services. An ISA server 2000 function takes the following parameters:

- **Server** – The NetBIOS name, DNS name or the IP address of the ISA server you want to monitor
- **Type of ISA server installation** – Choose Integrated/Firewall or Cache mode.

### File Existence

File Existence

File (UNC path)

\\GFITEST\\GFINetMon\Server\Help\Order.txt

**Existence**

- Check for existence only
- File must contain the following string (not case sensitive):

  ```
  www.gfi.com
  ```

**Log On**

- Log on with same account as service account [default]
- This account:
- Password:

**Note**

The file must be entered in UNC (Universal Naming Convention) format, i.e. `\\server\\sharename`. By default, the file will be checked for existence only. To search in a file for a pattern, select the `File must contain the following string` option. Click here to load a sample.
GFI Network Server Monitor can monitor for the existence of a file. This is particularly useful in situations where results of scheduled batch jobs need to be checked. In many organizations, batch jobs run at night and produce logging information; GFI Network Server Monitor can check this logging information and analyze it. It can check the existence of the file, and also or search for patterns/strings in the file itself.

A File Existence function takes 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 / File must contain string** – In case of ‘Check for Existence only’, only the existence of the file is checked. In case of ‘File must contain string’, the content of the file is checked for specific contents;
- **Log on with same account / Log on with other account** – Choose the account to be used by the GFI Network Server Monitor service to logon the remote server. By default, the service account of the GFI Network Server Monitor service is used.

As an administrator, you may want to get an alert when certain files are getting too large (for example log files). GFI Network Server Monitor can check for file sizes of particular files on local and remote machines.

You can use this function to monitor .pst file size on a user’s computer, and ensure that it does not get too large.

A File Size function takes the following parameters:

- **File** – the file name in UNC (‘Universal Naming Convention’) format. For instance: `\server01\public\docs\sales.doc`;
- **Size limit** – maximum file size in KB.
GFI Network Server Monitor can check the availability of FTP sites on port 21.

If GFI Network Server Monitor is behind a proxy server, you can configure GFI Network Server Monitor to go through the proxy server. In addition, you can pass credentials (username and password) to access the actual FTP site if the FTP server requires it.

An FTP monitor function takes the following parameters:

- **Use FTP site authentication** – A flag to indicate whether authentication is required for the ftp site or not. If authentication is required, ‘Website Account’ and ‘Website Password’ must be provided;
  - Account – A valid account on the ftp site;
  - Password – A valid password for the account;
- **Use a Proxy server** – A flag indicating whether the ftp 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.
GFI Network Server Monitor can check the availability of HTTP and HTTPS sites, on default ports (i.e.: 80 and 443).

If GFI Network Server Monitor is behind a proxy server, you can configure GFI Network Server Monitor to go through the proxy server. In addition, you can pass credentials (username and password) to access the actual HTTP site if the HTTP server requires it.

An HTTP/HTTPS function takes 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 string – In case of ‘Check for Availability only’, only the availability of the site is checked. In case of ‘Page must contain string’, the content of the URL is checked for specific contents;
- Use Web 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

![Screenshot 26 - ICMP/Ping monitor function properties]

The ICMP Ping monitor function checks a remote host for availability. Local hosts should normally respond to ping requests within milliseconds.

GFI Network Server Monitor checks servers for availability by sending ICMP Echo commands and waiting for the response. An ICMP timeout failure doesn't necessarily mean that the remote host is actually functioning beyond its ability to echo packets.

An ICMP/Ping function takes the following parameters:
• Hostname or IP address – 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 for each reply – Maximum number of milliseconds it may take before a response is received;
• Number of Echo requests to send – Maximum number of milliseconds it may take before a response is received.
Note: On a congested network it may take up to 3 seconds or longer to receive an echo packet from the remote host. If the timeout is set too low under these conditions, it will appear that the remote host is not reachable. If your network can be congested at times, set the timeout level accordingly.

**IMAP Mail Server availability**

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

An IMAP Mail Server rule takes 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 – Checks the response. (Only if a send command is configured) The default response for IMAP servers includes: ‘IMAP’;
- Timeout – Number of milliseconds before the function will timeout. 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.
MS SQL / ADO Database

GFI Network Server Monitor uses ADO to check availability of Microsoft SQL databases. ADO means: ActiveX Data Object. It provides a DSN-less connection to a variety of databases, like MS SQL and MS Access.

An MS SQL / ADO function takes the following parameters:
- ADO Connection String – the ADO connection string (for instance: DRIVER=Microsoft Access Driver (*.mdb); DBQ = \DELL01\AXNetMon\Server\Samples\Northwind.mdb);
- Login required – indicates whether login is required or not;
- Account – the account name (only if logon to the database is required);
- Password – the password (only if logon to the database is required).

Novell NDS

GFI Network Server Monitor checks different kinds of Directory Services. Novell NDS is one of them.

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

To add a Novell NDS function, do the following:
1. Add a new VBScript rule;
2. Click on the Browse button and choose the ads.vbs file;
3. View the file by clicking on the View button;
4. Choose the appropriate VB function and enter this name in the Function Name field;
5. Add the appropriate parameters. All string parameters should be enclosed in " " marks;
NNTP News Server availability

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

An NNTP News Server Availability function takes 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 – Checks the response. (Only if a send command is configured). The default response for NNTP servers includes: ‘200’;
- Timeout – Number of milliseconds before the function will timeout. 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 availability

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. GFI Network Server Monitor also uses NTP to check availability of internal and external time sources.

An NTP function takes the following parameters:

- Time Server – Hostname or IP address of the time server;

ODBC Database

GFI Network Server Monitor uses ODBC to check availability of a variety of databases. Most major database systems support ODBC, including: Microsoft SQL Server, Microsoft Access, Microsoft Excel, Oracle, FoxPro, Paradox, SyBase, Informix, OpenIngres, InterBase, Progress, IBM LANDP, DB2 and AS/400.
To monitor a database via ODBC, you must first setup a System DSN entry to the database you wish to monitor on the server running GFI Network Server Monitor. To do this:

1. Go to Administrative tools > Data Sources (ODBC). This will launch the ODBC administrator.

2. Now go to the ‘System DSN’ tab and click ‘Add’. (It is important that you select ‘System DSN’ and not ‘User DSN’ otherwise the service will not have access to it.). Select the appropriate driver for the database you wish to monitor.

3. In the ODBC setup dialog, specify a data source name and select the database you wish to monitor. In this example we have used the ‘Northwind’ database, which is included in the samples subdirectory of GFI Network Server Monitor. Click OK to add the data source.

4. After you have configured the ODBC data source, you can enter it in the ODBC monitor function. Specify the ODBC data source name in the ODBC DSN Name box. If a user name and password are required to access the database, specify this also.
Note: This check requires the installation of SQL*Net (Included with Oracle) on the GFI Network Server Monitor machine.

GFI Network Server 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.

GFI Network Server 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 function takes the following parameters:

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

A Database-Oracle Logon/Logoff function takes 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.
POP3 Mail Server availability

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

A POP3 Mail Server monitor function takes 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, a command can be sent. By default, no command string will be sent;
- **Response must include string (not case sensitive)** – Checks the response. (Only if a send command is configured) The default response for POP3 servers is: "+OK POP3;"
- **Timeout** – Number of milliseconds before the function will timeout. 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.

**Printer Availability**

Note: This monitor function requires WMI to be installed on the computer running the GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript, which uses WMI, with the parameters you specify in the monitor function setup screen. WMI is only available on Windows 2000 and
higher machines, so this monitor function can only be used if both the GFI Network Server Monitor machine and the machine to be monitored are running Windows 2000 or higher.

To run this check, you must configure the printer to be monitored as a network printer on the machine running GFI Network Server Monitor and ensure that the name that you have configured is entered in the Printer name field.

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.

GFI Network Server Monitor checks printers for availability by checking their 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 to be malfunctioning.

A Printer Availability rule takes the following parameters:

- Print server – The name of the server where the print server is installed;
- Printer name – Enter printer name as you have configured it on the machine running GFI Network Server Monitor. (You must configure the printer as a network printer on the GFI Network Server Monitor machine)
Process

Note: This monitor function requires WMI to be installed on the computer running the GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript, which uses WMI, with the parameters you specify in the monitor function setup screen. WMI is only available on Windows 2000 and higher machines, so this monitor function can only be used if both the GFI Network Server Monitor machine and the machine to be monitored are running Windows 2000 or higher.

GFI Network Server Monitor enables you to check processes on local- and remote computers; if a process is active, a computer is considered available. If a process is not active, it is not available.

A Process monitor rule takes the following parameters:

- **Server** – The name of the server where the process is running;
- **Process** – The module name of the process, including the extension. For instance: alerter.exe, or explorer.exe.
GFI Network Server Monitor can monitor 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 monitor function takes the following parameters:

- **Server** – the NetBIOS name, DNS name or the IP address of the server you want to monitor;
- **Service** – The NT/2000/XP service that should be running;
- **Log on with same account / Log on with other account** – Choose the account to be used by the GFI Network Server Monitor service to check the remote server. By default, the service account of the GFI Network Server Monitor service is used.
GFI Network Server Monitor can check SMTP mail servers by establishing a connection on the remote TCP port (usually port 25) and doing a handshake. By handshaking, GFI Network Server Monitor can verify that the remote server’s SMTP protocol is working well.

A SMTP Mail Server rule takes 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, a command can be sent. By default, no command string will be sent;
- **Response must include string** – Checks the response. (Only if a send command is configured). The default response for SMTP servers includes: ‘200’;
- **Timeout** – Number of milliseconds before the function will timeout. 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.

In the "Host name" field, enter a valid host name, NetBIOS name or IP address. Computer names in UNC format (i.e. \server> notation) are also accepted. In the "Port" field, enter a valid TCP port number.

The default Timeout value is suitable for most connections. Change the timeout value for servers that have a slow response time.

Click here to load a sample.
SNMP function

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 function takes the following parameters:

- **Host** – Hostname or IP address of the server/device to be monitored;
- **Community** – The SNMP community string; Default: ‘public’;
- **OID (Object ID)** – The Object ID; the OID is a long numeric tag, used to distinguish each variable uniquely in the MIB and in SNMP messages;
- **OID Data type** – The OID Data type. The following types 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 operand: Equal To, Not Equal To, Less Than, Less or Equal To, Greater Than, Greater or Equal To. This operand is used to compare the actual SNMP value against the ‘OID Data Value’;
- **OID Data Value** – OID value that will be compared against the actual OID value, using the ‘OID Data must be’ operand.
GFI Network Server 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 rule takes 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, a command can be sent.
- **Response must include string** – Checks the response. (Only if a send command is configured).
- **Timeout** – Number of milliseconds before the function will timeout. 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.
UNIX RSH Shell Script

RSH is a client process that opens connections to rsh daemons, sends a command to be executed on the remote server and retrieves its output, both stdout and stderr. The connection is made on standard port 514 (tcp port for the shell/cmd protocol). GFI Network Server Monitor can launch scripts on Linux/Unix machines and analyze the output.

The following is required to launch a shell script on a remote UNIX/LINUX machine:

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

A RSH Shell Script rule takes the following parameters:

- Remote Host – IP address, DNS host name or WINS/NetBIOS address of the remote host on which to run the command;
- 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 timeout – Specifies the maximum number of milliseconds to wait for completion of the script; if the script takes longer, it will be terminated. Default value: 3000 milliseconds;
- Match following string – The string that should be present in stdout to consider the script execution as successful;
- Consider as success/error if stdout matches string – If string matches, consider the result as error or as success.

**Users & Groups**

![Screenshot 43 - User/Group membership monitor function properties](image)

GFI Network Server Monitor monitors groups and group membership. In case of unexpected members in certain groups (for instance: unexpected Domain Admins members), it will notify the network administrators. This function is an excellent way to detect intruders, since an intruder will frequently try to give him/herself administrator rights.

The User/Group membership function takes the following parameters:
- Domain – enter domain name
- Group – enter group name
- Allowed members – enter the members that are allowed to be a member of this group, separated by commas

**VBscript monitor function**

The VBscript function allows you to monitor almost anything, by writing your own function in VBscript. This is actually a lot easier than it sounds. For more information about writing custom scripts, see the
A VBScript function takes the following parameters:

- **VBScript Filename** – Path to the VBScript file. The script should contain a function as specified in the Function name field. This function should return True (-1) in case of success, or False (0) in case of an error;
- **Function name** – The function that GFI Network Server Monitor service will be calling to check the status of the server/device;
- **Parameter1** – 1st argument to the ‘Function name’ call;
- **Parameter2** – 2nd argument to the ‘Function name’ call;
- **Parameter3** – 3rd argument to the ‘Function name’ call;
- **Parameter4** – 4th argument to the ‘Function name’ call;
- **Parameter5** – 5th argument to the ‘Function name’ call.

Important: String parameters must be enclosed with the " marks.

Note

The VBScript file must be in UNC format (i.e., \server\share). Network Monitor will call the function as provided in the ‘Function name’ field. Click [here] to load a sample.
Configuring Notifications

Introduction

GFI Network Server Monitor supports e-mail notifications; Network notifications and SMS/Pager Notifications. Notifications are sent in two situations:

- When a Monitor Rule fails – after a configurable number of errors, the Monitor Rule is considered as failed. By default, only one notification is sent after a failure; if you want to be notified continuously after a failure, you should configure this from the Advanced button in the Monitor Rule Properties tab;
- When a Monitor Rule has recovered from the 'Failed' status – since GFI Network Server Monitor can recover a server/device, it can be useful to send an alert to the operator to tell him/her that the previous error is no longer there.

Notification Settings can be set globally for all monitor rules. To do this, select Notification settings from the Tools menu.

For all notification types - except pager notifications - you can configure a Global Recipient List. This list can be used in any monitor rule, which makes configuration of recipients much easier. However, you can still define a custom list of recipients for individual monitor rules.

E-mail Notifications

To use SMTP e-mail notifications, the GFI Network Server Monitor service must have access to an SMTP server to send out e-mails. It can be any SMTP compliant mail server.

NOTE: Many software products require IIS (Internet Information Server) to support e-mail. GFI Network Server Monitor doesn’t require IIS; it communicates directly with the SMTP server using the SMTP protocol.

GFI Network Server Monitor supports SMTP servers that require SMTP authentication, such as Microsoft Exchange. SMTP AUTH is a protocol that is used to verify that you are one of the users on the SMTP server. GFI Network Server Monitor is RFC 821 and RFC 822 SMTP AUTH compliant.
E-mail Notifications – Global settings

To configure global e-mail notification settings:


2. Your MUST configure an SMTP mail server. This is the server that will send out the actual notification messages to the recipients. You can specify an IP address (e.g. 10.0.0.1), a host name (e.g. mail.mydomain.com) or a NetBIOS name (like EXCHANGE01).

3. If your SMTP server requires authentication, click the authentication checkbox and provide a logon and password.

4. 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;

5. Configure the Global E-mail Recipient List. This list can be used for all monitor rules. The Global Recipient E-mail List makes configuration easier, because you don’t have to configure a separate list of recipients for each monitor rule; however, it is still possible to configure a separate list for each monitor rule;
6. Click on Format Message to edit the e-mail template and to enable/disable RTF (HTML) formatting.

7. Enable RTF (HTML) formatting to support HTML tags. If you switch on RTF formatting, you must use the `<br>` tag (or an alternative tag) to insert new lines.

8. To test the E-mail Notification Settings, click on the ‘Test’ button. The Network Server Monitor Engine will send an E-mail message using the configured settings.

Message Templates will be discussed later in this chapter.

**E-mail Notifications – Per Monitor Rule settings**
For each monitor rule, you can make the following configuration settings:

- Notify when server/device goes offline – when the server has a failure, a message is sent. Default: On;
- Notify when server/device goes online – when the server changes to Online status from Offline status, a message is sent. Default: Off;
- For both Online and Offline status changes, you can choose to use the Global E-mail Recipient List as configured in the General E-mail Notification Settings, or use a Custom E-mail Recipient List.

### Network Notifications

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

**Screenshot 48 Network Message global settings**

### Network Notifications – Global settings

To configure general network notification settings:

1. On the Tools menu, click Notification Settings and select the Network Messages tab;
2. Specify a Global Network Recipient List. This list can be used for all monitor rules. A Global Network Recipient List makes configuration easier, because you don't have to configure a separate list of recipients for each monitor rule; however, it is still possible to configure a separate list for each monitor rule;

3. Click on Format Message to edit the network message template. Please read the Message Template section about how to use message templates.

4. To test the Network Notification Settings, use the ‘Send a Test Message’ button. The Network Server Monitor Engine will send an E-mail message using the configured settings.

**Network Notifications – Per monitor rule settings**

For each monitor rule, you can configure the following:

- Notify when server/device goes offline – when the server has a failure, a message is sent. Default: On;
- Notify when server/device goes online – when the server changes to Online status from Offline status, a message is sent. Default: Off;
- For both Online and Offline status changes, you can choose to use the Global Network Message Recipient List as configured in the General Network Message Notification Settings, or use a Custom Network Message Recipient List.

**SMS Notifications**

GFI Network Server Monitor can send SMS messages in two ways:

- Through an SMSC (Short Message Service Center). This requires a normal Hayes compatible modem, connected to the server where the Network Monitor Engine is running. When there’s a failure, GFI Network Server Monitor uses the modem to dial-in to the SMSC provider and deliver the actual SMS message(s); Most countries have one or more SMSC service providers.
- Through a GSM phone or GSM modem, connected to the server by serial cable, Infrared or Bluetooth. The GSM phone must be capable of processing AT+C commands (most modern GSM phone do).
SMS Notification – Global settings

To configure global SMS notification settings:

1. On the Tools menu, click Notification Settings and select the SMS/Pager tab;
2. Choose either ‘Send SMS through SMSC provider’ or ‘Send SMS though mobile phone’.
3. If you selected to send SMS through a GSM phone or modem, click on configure. This brings up the GSM modem settings dialog. Select the com port on which you have connected the GSM phone or
modem. Leave other settings as default, unless you are sure that they need to be changed. Click OK.

4. If you selected to send SMS via an SMS service provider, click on configure. This brings up the SMSC settings dialog. Now click on ‘Select’ to select your provider. (if your SMS provider is not listed see the section in this chapter about editing SMSC providers) Then configure dial properties: Specify tone or pulse, a dial prefix if required and the number of redial attempts. The Dial-string box will show the exact string that will be dialed. In addition configure the modem settings: Specify com port. Leave initialization string and flow control setting as default, unless you are sure they have to be changed.

5. Specify a Global Network Recipient List. This list can be used for all monitor rules. A Global Network Recipient List makes configuration easier, because you don’t have to configure a separate list of recipients for each monitor rule; however, it is still possible to configure a separate list for each monitor rule;

6. Click on Format Message to edit the network message template. Please read the Message Template section about how to use message templates.

7. To test the Network Notification Settings, use the ‘Send a Test Message’ button. The Network Server Monitor Engine will send an E-mail message using the configured settings.

NOTE 1: You can turn on modem logging for the Network Monitor Engine. To do so, you must enter a valid file name in the following registry entry:
HKLM\Software\GFI\Network Monitor\ModemLogFile

NOTE 2: SMSC providers request a particular connection speed. Therefore this is configured in the provider list.

NOTE 3: The required recipient number’s format depends on the provider (when using SMSC) or on GSM (when using local GSM
phone). You must do some trial and error to find out the right format. For example, if you live in the UK (+44), you should try:

12345678
4412345678
004412345678

**SMS Notification Settings - Monitor Rule**

For each monitor rule, you can configure the following:

- **Notify when server/device goes offline** – when the server has a failure, a message is sent. Default: On;
- **Notify when server/device goes online** – when the server changes to Online status from Offline status, a message is sent. Default: Off;
- For both Online and Offline status changes, you can choose to use the Global SMS Recipient List as configured in the General SMS Notification Settings, or use a Custom SMS Recipient List.

**Creating/Editing SMSC providers**

Note: This section is only applicable for advanced users. We can not guarantee that GFI Network Server Monitor will work with any SMS provider. Ensure that you obtain the correct information from your SMS service provider first.
GFI Network Server Monitor includes an extensive list of SMS service providers. However, it maybe necessary to change the SMS service provider settings from time to time, or it maybe that the SMS service provider that you wish to use is not listed. In this case you have to add/edit an SMSC provider entry.

To add/edit an SMSC provider:

1. Select Tools > Notification settings and go to the global SMS notifications tab
2. Click on the Configure button in the ‘Send SMS via SMS service provider section’
3. Click on the ‘Select’ button next to the provider section. This brings up the SMSC provider list.

4. Click on Add or Edit to Add/Edit an SMSC entry. Specify the following settings:
   - **Country**: Specify the country of the provider
   - **Provider**: Specify the provider name
   - **Dial-in number**: Specify the number to which the modem must dial.
- Data format: Specify the data format. Obtain this from your service provider.
- Speed: Specify the speed at which the data must be sent. Obtain this number from your SMS service provider.
- Protocol: Choose between the TAP (Telecator Alphanumeric Protocol) and UCP (Universal Computer Protocol). TAP is the more used protocol, although you should ask your SMS service provider which protocol they use.
- Optionally you can specify a password and any comments.

5. Click OK to add the service provider.

**Message Templates**

Notification message text can be customized by editing the message templates used by GFI Network Server Monitor. This can be done by clicking on the Format Message button in either the Global Email, Network Message or SMS notification settings tabs.

![Screenshot 55 - Editing the SMS message template](image)

Each message template supports the use of variables. Variables are substituted each time a message is sent out. Variables must be enclosed between `<%` and `%>` strings, for example: `<% DATE %>`. The following variables can be used:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE</td>
<td>The date the event occurred</td>
</tr>
<tr>
<td>TIME</td>
<td>The time the event occurred</td>
</tr>
<tr>
<td>DISPLAYNAME</td>
<td>Name of the Monitor Rule (can be changed in the general settings of the rule)</td>
</tr>
<tr>
<td>SERVER</td>
<td>Name of the server/device that is being checked</td>
</tr>
<tr>
<td>RESULT</td>
<td>The result of the event</td>
</tr>
<tr>
<td></td>
<td>- Success;</td>
</tr>
<tr>
<td></td>
<td>- Failure;</td>
</tr>
<tr>
<td></td>
<td>- Maintenance;</td>
</tr>
<tr>
<td></td>
<td>- On Hold;</td>
</tr>
<tr>
<td></td>
<td>- Unknown.</td>
</tr>
</tbody>
</table>
### OCCURRENCE

The occurrence:
- Recovery;
- Failure;
- Maintenance;
- On Hold;
- Unknown.

In most cases, this variable is the same as the RESULT variable. The only exception is when occurrence is ‘Recovery’, in this case the result variable is ‘Success’.

### EXPLANATION

Detailed description of the result of the event

#### Message Template Example

Example of a message template:

Message from GFI Network Server Monitor, `<% DATE %> `<%TIME %>

Item: `<% DISPLAYNAME %>`
Result: `<% RESULT %>`
Explanation: `<% EXPLANATION %>` Message from GFI Network Server Monitor, `<% DATE %> `<%TIME %>

NOTE: Using new lines in SMS/Pager Message Templates is NOT recommended. Most GSM phones don’t know how to handle new lines and will display bad characters.
Remote web monitor

Introduction to the remote web monitor

The remote web monitor allows you to check rule status from anywhere using a web browser. Two types of web page views have been created:

1. A normal view for use with a ‘normal sized’ computer screen
2. A view optimized for mobile device access, such as a mobile phone, blackberry or other handheld computing device.

To view these reports, you can connect with your web browser to the machine running GFI Network Server Monitor, on port 11694 (this can be changed).

By default, GFI Network Server Monitor includes a small footprint web server, which avoids you having to install and configure IIS to show the GFI Network Server Monitor status screens. This option is fine for intranet access.

However, if you wish to have more advanced security, we do recommend using Microsoft IIS as the web server to show the rule status. Below follows a detailed procedure on how to configure IIS to serve up the rule status pages.

Normal web monitoring page

This page is for use with regular screens and shows detailed information about all the rules currently being monitored and their current state.

The URL to access the normal web monitoring page:
http://<machine name>:11694/index.html
Mobile/handheld device monitoring page

This page is optimized for viewing from mobile/handheld devices, such as mobile phones, organizers and blackberrys, and thus the view has been made much smaller.

The URL to access the mobile device monitoring page:
http://<machine name>:port/mobile.html
Configuring the remote web monitor

To enable the remote web monitor:
1. Go to the Tools menu in the GFI Network Server Monitor manager and select ‘Remote Monitor’
2. Tick the ‘Enable remote monitoring’ option in the remote monitor dialog.

This will cause the GFI Network Server Monitor service to start logging the rule status to an XML file, from where either the internal web server or IIS can be used to display the data as an HTML page on either a normal screen or on a mobile device screen.
Using the internal web server

For easy remote monitoring from anywhere on your network, an internal web server has been included, avoiding the need to configure a web server. By default the internal web server is enabled and listens on port 11694.

Before you can start using remote monitoring via the internal web server, you need to create the users that are allowed to view the remote monitor page. To do this, click ‘Add’ and specify user name and password. You can specify up to 100 users.

When you connect to the remote web monitor, you will be asked for these credentials.

Configuring IIS as the web server

Using IIS as the web server gives you more advanced authentication features and the possibility to secure the connection via SSL. The integration with IIS is very straightforward. GFI Network Server Monitor updates an XML file, from which the 2 views are rendered. These files are stored in the GFI Network Server Monitor\Server\web folder. You need to create a virtual directory in IIS, which points to the GFI Network Server Monitor\Server\Web folder. To do this:

1. Start up Internet Services Manager, right click on the Web Site node, and from the popup menu select New – Virtual Directory.
2. This will start the Virtual Directory Creation Wizard. Click 'Next' to continue. Now you need to enter an alias for the virtual directory. In this case it is nsmremotemonitor, but you can enter whatever name you like, as long as it follows the folder naming conventions used in Microsoft Windows.

3. Now enter the path where the content is located. Select browse, and select the server\web folder in the GFI Network Server Monitor installation path.
4. Next we need to set the access permissions. Tick ‘Read’ only. Do not tick any of the other check boxes. Now click ‘Next’ to finish the Virtual Directory Creation Wizard.

5. Right-click on the newly created virtual directory, located under the web root of your web site server and select properties.

6. In the Virtual Directory tab of the properties dialog, tick the ‘Read’, the ‘Log Visits’ and the ‘Index this resource’ check boxes.

7. Press OK to close the properties dialog. The Virtual Directory has been set-up and you can now test access to it.
Securing the Remote Monitor

It is important to setup proper authentication and security for this web server and virtual directory. There are three ways to secure the Remote Monitor. These are Basic Authentication, Digest and Integrated Windows Authentication. Integrated Windows Authentication is the preferred choice in an Active Directory environment, because it makes the authentication process seamless, since initially it does not prompt users for their user name or password information. It uses the current Windows user information on the client computer for authentication, instead. If you are installing GFI Network Server Monitor on a DMZ, you must use Basic authentication.

The following steps show how to secure access to the Web based remote monitor.

1. Open up Internet Services Manager. Right click on the NSM Remote Monitor virtual directory under your server web site and select properties.


3. Select the Documents tab and remove all the default documents. Add the following default document 'index.html'.


5. Select Integrated Windows authentication (recommended if installed on the internal network) OR Basic Authentication check box (if installed in the DMZ). Ensure Anonymous access is deselected.
If using Integrated Windows authentication, then authentication will occur against Active Directory. This means you do not need to configure additional users. If you use basic authentication, authentication will occur against the local user database on the machine. In this case you must create user names and passwords on that local machine. For more information on securing IIS, please review the IIS documentation.

**Be sure not to allow anonymous access!**

6. Now restrict access to the pages by using NTFS permissions. Open up Explorer and navigate to the web folder in the GFI Network Server Monitor installation path. Right click on the 'web' sub folder and select properties and then the Security tab.
7. Add / remove the users / groups you want to allow access to the Remote Monitor. To allow access only to users forming part of the administrators group you would set the security tab as in the screenshot. Click OK. You have now secured the remote monitor.
Introduction to reporting

GFI Network Server Monitor logs rule status changes to a Microsoft access database, from which you can run reports to analyse network up-time.

GFI Network Server Monitor currently includes two reports:

- Detailed Availability Report;
- Summary Availability Report.

Reports can be outputted to HTML, to CSV or to XML format. The latter reports allow for easy analysis by other programs.

Detailed Availability Report

The Detailed Availability Report gives an overview of all state changes for a particular time interval. The report also shows how long the server/service was in each particular state. Using this report you can easily determine up time or downtime. To generate a new Detailed Availability Report

1. Start the GFI NSM reports application from the GFI Network Server Monitor program group. The reports wizard will start up. Select Next to continue.
2. Select Availability – Detailed Report

3. Specify the report interval, i.e. the period of time that you wish to have the report on.

4. Now specify whether you want the report to include all the monitor rules, or just a subset of these rules.
5. Now specify the format of the report. Use the CSV or XML format to do further processing on the report: You can import the report into Excel and make more advanced calculations on the data.

**Summary Availability Report**

The Availability Summary Report provides an overview of the amount of time that a server was in a certain state, during a specific time interval. The states are: ‘up’, ‘down’, ‘maintenance’, ‘on hold’ and ‘unknown’. The process of generating a new Availability Summary Report is identical to the Availability Details report.
Screenshot 72 - The availability summary report

<table>
<thead>
<tr>
<th>Server</th>
<th>Up</th>
<th>Down</th>
<th>Uncertain</th>
<th>Dependent unavailable</th>
<th>Maintenance</th>
<th>On hold</th>
<th>Not monitored</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAILSERVER - KMP Proig</td>
<td>2 hrs 7 min 00 min</td>
<td>0 min</td>
<td>0 min</td>
<td>0 hrs 0 mins</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAILSERVER - SMTP Mailserver</td>
<td>2 hrs 7 min 00 min</td>
<td>0 min</td>
<td>0 min</td>
<td>0 hrs 0 mins</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAILSERVER - IPD Mailserver</td>
<td>2 hrs 7 min 00 min</td>
<td>0 min</td>
<td>0 min</td>
<td>0 hrs 0 mins</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Report generated by GFI Network Server Monitor.
Writing your own monitoring functions

Introduction

Note: GFI Support can not assist you in the writing and debugging of custom scripts. You must be familiar with VBscript to write your own functions and you must debug them yourself.

GFI Network Server Monitor is designed to let operators write their own monitor functions and use them in the product. GFI uses VBScript because it is the most popular scripting language in Windows environments.

GFI Network Server Monitor uses VBscript itself to perform a number of checks. In fact, during installation, five VBScript files are installed:

- ads.vbs – includes monitor functions based on ADSI (Active Directory Service Interfaces);
- exchange.vbs – includes monitor functions that can check Exchange 2000/2003 servers;
- hardware.vbs – includes hardware related monitor functions;
- os.vbs – includes Operating System related monitor functions;
- sample.vbs – includes some sample functions.

Writing a script/function

GFI Network Server Monitor functions should always return:

-1 (True); Return -1 in case the Monitor Function 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 Monitor Function 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 Monitor Function 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;

It’s very easy to write your own monitor functions in VBScript. Use the following guidelines when writing a new function:

- The routine must be a Function, not a Sub;
- The Function must return True (-1), False (0) or Unknown (1);
- Optionally, use the EXPLANATION system variable to add your own explanation to the result of the function; this EXPLANATION is shown in the client program each time the check is made;
• All variables must be 'dimmed', except EXPLANATION. EXPLANATION is an GFI Network Server Monitor system variable and is already dimmed by the GFI Network Server Monitor service.

The function must be written according to the following template:

```vbs
Const retvalUnknown = 1
Function Function_i( var1, var2, ..., varn )
    If( Not Pre-condition ) Then
        EXPLANATION = "Unable to determine..."
        Function_i = retvalUnknown
    Else
        If( condition ) Then
            EXPLANATION = "Yes it is true because ...
            Function_i = True
        Else
            EXPLANATION = "No it’s not true because ...
            Function_i = False
        End If
    End If
End Function
```

where Function_i is an arbitrary name for the function.

You can save this function in either one of the standard VBS files (i.e. ads.vbs, exchange.vbs, hardware.vbs, os.vbs or sample.vbs), or in a new VBScript file. In case of a new file ensure that your VBS file is accessible via the GFI Network Server Monitor Share.

---

**Adding a monitor function written in VBScript**

After you have written a monitor function in VBScript, you must add it in the Network Server Monitor Manager as a rule. To do this:

1. Create a new rule. In the monitor rule general tab, select ‘VBscript’ in the Monitor function drop down list box.
2. The VBscript monitor function properties dialog will appear. Specify the location of the VBscript file in UNC format.

3. Now specify the VBscript function name – This is the function that GFI Network Server Monitor service will be calling to check the status of the server/device. This function should return True (-1) in case of success, or False (0) in case of an error;

4. Optionally specify the up to 5 parameters:
   - Parameter1 – 1st argument to the ‘Function name’ call;
   - Parameter2 – 2nd argument to the ‘Function name’ call;
   - Parameter3 – 3rd argument to the ‘Function name’ call;
   - Parameter4 – 4th argument to the ‘Function name’ call;
   - Parameter5 – 5th argument to the ‘Function name’ call.

**WMI (Windows Management Instrumentation)**

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

WMI is part of the Windows 2000/2003 operating system; it’s not part of NT4. For NT4, please download the file from the Microsoft website; WMI for NT4 is available for free.

GFI has collected more than a hundred WMI samples. You can use these samples as a base for new monitor functions that you write yourself. You can find them on the GFI website.
**ADSI (Active Directory Service Interfaces)**

GFI Network Server Monitor can check several Directory Services including Active Directory, NTDS (NT4 SAM database) and Novell directory services.

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

If you plan to write monitor functions based on ADSI (Active Directory Service Interfaces), be sure you have ADSI installed on the GFI Network Server Monitor server and on the server that you want to monitor. ADSI allows you to access Windows 2000/2003 Active Directory, but also NT4 User information from the SAM database, and other User Databases such as Novell Bindery.

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

GFI includes a sample script that uses ADSI, called ads.vbs. In addition, GFI provides some sample ADSI scripts on the website. You can use these samples as a base for new monitor functions that use ADSI.
Advanced features

Configuring Logging

GFI Network Server Monitor logs all activity to a log file. By default, logging is enabled and the log file is written to:
<installation directory>\server\logs.

You can change the directory or switch off logging from the Logging tab of the Options dialog, located under the Tools menu.

Configuring dependencies

Using dependencies, you can avoid receiving a flood of notification messages when 1 server/service, on which other servers depend, malfunctions.
To configure dependencies:
1. From the Tools menu, select dependencies.
2. Select the rule on which other servers/services depend.
3. Now click on the ‘Add’ Button to add the dependant rules.

Configuring Global Maintenance Periods

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

During these intervals, you probably do not want to receive any alerts from GFI Network Server Monitor – after all you are already aware of the fact that the servers are down. To avoid receiving alerts during the maintenance periods, you can define ‘Maintenance Periods’, during which GFI Network Server Monitor will not send any alerts or undertake any actions.

Maintenance periods can be configured globally (for all monitor rules) or at the Monitor Rule level. The Maintenance Period can be configured as a one off, or as recurrent period.
To configure Maintenance Periods:
1. From the Tools menu, select Options and go to the Maintenance Periods tab;
2. Choose either Never, Only Once or Day of Week.
• ‘Only Once’ - provide start date and time, and number of hours the computer and devices will be unavailable;
• ‘Day of Week’, provide the days of the week that the computers and devices will be unavailable as well as start time and number of hours the servers will be unavailable.

Setting Default Rule Options

You can configure Default Rule options in order to save time when creating rules or when you want to make the same change to all rules.

To configure default rule options:
1. From the Tools menu, select ‘Options’.
2. Set the default rule options in the Defaults tab.

Monitoring defaults

Monitor every x seconds/minutes/hours/days – specifies at which interval the check will be performed. Default value is 2 minutes.
Consider failure after x consecutive errors – specifies the number of consecutive errors that must occur before a check is considered as Failed. Default value is 3.

Notification defaults

You can have an Email, Network Message and/or SMS notification sent for the following conditions:
- Notify when server/device goes offline – when the server has a failure, a notification is sent. Default: On;
- Notify when server/device goes online – when the server changes to Online status from Offline status, a notification is sent. Default: Off;

**Notification Frequency Defaults** - Specifies how often a notification should be sent after a failure. By default, a notification is sent only once after failure. However, you can configure to be notified every x minutes after failure;

**Action Frequency Defaults**
Specifies how often actions (restart service, restart computer, run program) should be triggered after failure. By default, an action is triggered only once after failure; however, you can configure that an action is triggered every x minutes after failure;

‘Apply To Existing Rules Now’: Default entries only apply when monitor rules are created; they don’t affect existing monitor rules. You can apply new default settings to all monitor rules by pressing the ‘Apply To Existing Rules Now’ button.

---

**Import, Export and Clear configuration settings**

The GFI Network Server Monitor configuration consists of two parts
- Monitoring Rules – all monitoring rules and monitoring properties;
- Global configuration data – this data is configured independent from the monitoring rules, and contains defaults, global recipient lists, maintenance hours, and so on.

All configuration data is stored in one file: CONFIG.AMF. and is located in de \INSTALL-DIR>\SERVER\CFG\ directory

**Import configuration settings**

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

1. On the File menu, click ‘Import and Export’ and choose Import configuration;
2. The Import configuration wizard will ask if you wish to backup your configuration data first. This is recommended.

3. Now you specify whether you want to import only the rules, or both the rules and the program settings. Click ‘Browse’ to specify the name of a previously exported configuration file.

4. Click Next. The configuration data will be imported. Click Finish to exit the wizard.

   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 including global configuration settings (such as mail server, default scan time, etc.) as well as all monitor rules.
To export a configuration:
1. On the File menu, click ‘Import and Export’ and choose Export configuration
2. In the File name box, enter a name for the new export configuration file;
3. Click Save.

**Clear configuration settings**

The Clear configuration function clears the existing configuration. The GFI Network Server Monitor Manager will ask you to save the current configuration before you clear it.

To clear a configuration:
1. On the File menu, click ‘Import and Export’ and choose Clear;
2. The program will ask if you want to export the current configuration;
3. After the optional export, it asks you if you’re sure to clear the configuration. Press Yes.

**Renaming computers**

If you want to rename the computer where the GFI Network Server Monitor Engine is installed on, you have to:
1. Export the configuration.
2. Stop the Network Monitor Engine;
3. Change the following registry entries:
   - HKLM\Software\GFI\Network Monitor\Engine0
   - HKLM\Software\GFI\Network Monitor\Engine0Root
   - HKLM\Software\GFI\Network Monitor Manager\Engine0Root
   - HKLM\Software\GFI\Network Monitor Manager\Engine0Root;
4. Start the Network Monitor Engine;
5. 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.
6. On other PCs in the network that have the Manager application installed, make changes to these two registry entries:
   - HKLM\Software\GFI\Network Monitor Manager\Engine0Root
   - HKLM\Software\GFI\Network Monitor Manager\Engine0Root;
Troubleshooting

Introduction

The troubleshooting chapter explains how you should go about resolving issues you have. The main sources of information available to users are:

1. The manual – most issues can be solved by reading the manual.
2. The GFI knowledgebase – accessible from the GFI website.
3. The GFI support site.
4. Contacting the GFI support department by email at support@gfi.com
5. Contacting the GFI support department using our live support service at http://support.gfi.com/livesupport.asp
6. Contacting our support department by telephone.

Knowledgebase

GFI maintains a knowledgebase, which includes answers to most common problems. If you have a problem, please consult the knowledgebase first. The knowledgebase always has the most up-to-date listing of support questions and patches.

The knowledgebase can be found on http://kbase.gfi.com

Request support via e-mail

If, after using the knowledgebase and this manual, you have any problems that you cannot solve, you can contact the GFI support department. We recommend doing this via e-mail.

The Troubleshooter, included in the program group, generates automatically a series of files needed for GFI to give you technical support. The files would include the configuration settings etc. To generate these files, start the troubleshooter and follow the instructions in the application.

In addition to collecting all the information, it also asks you a number of questions. Please take your time to answer these questions accurately. Without the proper information it will not be possible to diagnose your problem.

Then go to the support directory, located under the main program directory, ZIP the files, and send the generated files to support@gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.
Ensure that you have registered your product on our website first, at http://www.gfi.com/pages/regfrm.htm!

Request support via web chat

You may also request support via Live support (web chat). You can contact the GFI support department using our live support service at http://support.gfi.com/livesupport.asp

Ensure that you have registered your product on our website first, at http://www.gfi.com/pages/regfrm.htm!

Request support via phone

You can also contact GFI by phone for technical support. Please check our support website for the correct numbers to call, depending on where you are located, and for our opening times.

Support website:
http://support.gfi.com

Ensure that you have registered your product on our website first, at http://www.gfi.com/pages/regfrm.htm!

Web Forum

User to user support is available via the web forum. The forum can be found at:
http://forums.gfi.com

Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds.
To subscribe to our build notifications, go to:
http://support.gfi.com
Index

A
Action frequency 22
administrator credentials 11
ADSI 7, 16, 67, 70

B
Batch 20

C
CPU usage 6, 7, 27

D
database 5
Directory size 6
Disk drive 6
Disk space 6, 28, 29
DNS server 6, 15, 30

E
Event ID 6, 31, 32
Event Log 30, 31
Exchange 5

F
File existence 6, 33
File size function 6
FTP 6, 34, 35

H
HTTP function 6

I
ICMP ping 6

L
License 8, 9

M
Message Templates 20, 57, 64, 65

N
Network Monitor Engine 5, 8, 24, 49, 59, 61, 81
Network Monitor Manager 8, 78, 81
NNTP 6, 15, 40
Notification frequency 22
Novell 7, 39, 70
NTP 6, 15, 41

O
ODBC 5
ORACLE 5

P
Pager 17, 19, 55, 60, 65
POP3 6, 15, 44
POP3 server 6, 44
Printers 15, 45
Processes 15

Q
Quick Configuration 12

R
Reporting 7
RSH 7, 16, 51

S
Server maintenance periods 22
SMSC providers 61, 62
SMTP server 6, 48, 55, 56
SNMP 6, 16, 24, 49
SQL 5, 15, 39, 41, 43
System requirements 9

T
TCP 6, 16, 38, 40, 44, 48, 50

U
UDP 6, 16
UNIX 5, 7, 16, 51

V
VBScript 7, 16, 17, 20, 39, 53, 67, 68

W
WMI 7, 16, 27, 28, 30, 32, 44, 46, 52, 69

X
XML 7