Performance Endpoints 5.1

Windows Millenium (Me)

April 2006

Legal Notice

Contents

About This Guide

This guide provides practical information about the free Performance Endpoint software NetIQ Corporation provides in association with its Systems Management products. It explains installation and configuration for all the endpoint platforms supported by NetIQ AppManager Networks Response Time and VoIP Quality modules, NetIQ Vivinet Assessor, and NetIQ Vivinet Diagnostics. You can also download individual endpoint guides in PDF format from the Internet at www.netiq.com/download/endpoints.

Intended Audience

This guide contains information about Performance Endpoint software for users of NetIQ AppManager, Vivinet Assessor, and Vivinet Diagnostics.

Using This Guide

Depending on your environment and your role as a user of the aforementioned NetIQ products, you may want to read portions of this guide selectively. It contains the following chapters:

- Chapter 1, "Introduction to Performance Endpoints," describes the software and hardware requirements and the supported functions of the Performance Endpoints, version 5.1.
- Chapter 2, "Endpoint Initialization File," discusses the functions of the endpoint initialization file, which is installed with each Performance Endpoint.

- Chapter 3, "Microsoft Windows Me," installation, configuration, and operation of the Performance Endpoint software for Microsoft Windows Millennium Edition (Me).

In addition to these chapters, an index is provided for your reference.

Conventions Used in this Guide

The following conventions are used in this guide:

- `Fixed-width font` is used for source code, program names or output, file names, and commands that you enter at the command line.
- An *`italicized`* fixed-width font is used to indicate variables.
- **Bold text** is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- *Italics* are used for book titles.

Complementary NetIQ Products

NetIQ Corporation is a leading provider of intelligent, e-business management software solutions for all components of your corporate infrastructure. These components include servers, networks, directories, Web servers, and various applications.

NetIQ provides integrated products that simplify and unify directory, security, operations, and network performance management in your extended enterprise. NetIQ provides the following categories of products:

- **Systems Management** NetIQ Systems Management products provide control and automation for monitoring the performance and availability of your critical servers, applications, and devices; tools for diagnosing and

analyzing system operation; and extensive network monitoring capabilities to provide a complete, end-to-end management solution for the enterprise. These products enable you to pinpoint existing and potential server and network problems and resolve those problems quickly and effectively.

- **Security Management** NetIQ Security Management products enable you to administer, assess, enforce, and protect all aspects of security within your Windows environment. These products provide incident management and intrusion detection, vulnerability assessment, firewall reporting and analysis, and Windows security administration.
- **Smart Solutions for Windows Administration** NetIQ Smart Solutions for Windows Administration include tools for managing, migrating, administering and analyzing your Windows, Exchange, and SQL Server environments. These products include tools for setting and enforcing policies that govern user accounts, groups, resources, services, events, files, and folders, and products that automate time-consuming administration tasks.

Contacting NetIQ

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. For a complete list of our

partners, please see our Web site. If you cannot contact your partner, please contact our Technical Support team.

Telephone:	713-418-5678
Support:	support@netiq.com
Web site:	www.netiq.com/support

Chapter 1

Introduction to Performance Endpoints

This guide contains information about the Performance Endpoints, which are available for more than 15 different operating systems.

All the information you need to install, configure, and run the endpoints in your network is included here. In addition to topics discussing issues common to all the endpoints, this guide also contain information about each operating system, organized in separate chapters.

The following topics describe the software and hardware requirements and the supported functions of the Performance Endpoints, version 5.1.

- "Operating System and Protocol Stack Support" on page 2
- "Endpoint Capabilities" on page 2

The latest version of the endpoint software can always be downloaded free from the Internet. A single installable file is available for each supported operating system. Endpoints are available for downloading at www.netiq.com/download/endpoints.

You cannot run endpoint software from a CD-ROM; you must install it on a computer.

Operating System and Protocol Stack Support

The following table lists the software with which we have tested the Performance Endpoints for each operating system.

Endpoint	OS Version	TCP, UDP, RTP	IP Multicast Version
Cobalt RaQ3 (x86)	Kernel 2.0.32	Included	Kernel 2.0.32
HP-UX	HP-UX v10.10	Included	v10.10
IBM AIX	AIX v4.1.4	Included	v4.1.4
Linux (x86 and MIPS)	Kernel 2.0.32	Included	Kernel 2.0.32
Microsoft Windows Millennium Edition (Me)	Windows Me	Included	Included
Microsoft Windows 2000	Windows 2000	Included	Included
Microsoft Windows 2003 Server	Windows XP (32-bit)	Included	Included
Microsoft Windows XP	Windows XP (32-bit)	Included	Included
Sun Solaris for SPARC	Solaris v2.4	Included	v2.4
Sun Solaris for x86	Solaris v2.4	Included	v2.4

Endpoint Capabilities

The following table indicates which endpoints have been tested with and are supported by NetIQ products.

NetIQ Product	Vivinet Assessor	Vivinet Diagnostics	AppManager for Networks-RT	AppManager for VoIP Quality
Endpoint				
HP-UX	No	No	Yes	No
IBM AIX	No	No	Yes	No
Linux for Cobalt RaQ3 (x86)	Yes	Yes	Yes	Yes

NetIQ Product	Vivinet Assessor	Vivinet Diagnostics	AppManager for Networks-RT	AppManager for VoIP Quality
Endpoint				
Linux x86 (TAR)	Yes	Yes	Yes	Yes
Linux x86 (RPM)	Yes	Yes	Yes	Yes
Microsoft Windows Me/2000/XP/2003	Yes	Yes	Yes	Yes
Microsoft Windows Me/2000/XP/2003 (Web-Based)	Yes	No	No	No
Sun Solaris (SPARC)	Yes	Yes	Yes	Yes
Sun Solaris Endpoint (x86)	Yes	Yes	Yes	Yes

Chapter 2

Endpoint Initialization File

An endpoint initialization file is installed with each Performance Endpoint. With this file, you can do the following:

- Restrict the use of this endpoint to specific AppManager, Vivinet Diagnostics, or Vivinet Assessor Console.
- Control which access attempts are logged in an audit file.
- Change the filename of the audit file.
- Enable only particular protocols on this endpoint for setup connections.

On most operating systems, this file is named `endpoint.ini`. This file has the same format and structure on all the operating systems.

Here are the default contents of the endpoint initialization file. You can change these keywords and their parameters to tailor individual endpoints for your needs.

Keyword	Parameters
ALLOW	ALL
SECURITY_AUDITING	NONE
AUDIT_FILENAME	ENDPOINT.AUD
ENABLE_PROTOCOL	ALL

This file is an editable text file. There is a separate copy for each operating system. You might want to make changes to it once, before endpoint installation, which are then incorporated into all the installs for different sets of computers. You can modify this text file before installation by copying the endpoint installation directory for an

operating system to a hard drive (preferably a LAN drive), and then modifying the file before running the install from that drive.

We strongly recommend that you make any changes to your `endpoint.ini` files once, before you install any endpoints, as opposed to installing the endpoints and then going back to each of them and separately modifying each one.

ALLOW

This keyword determines which computers can run tests using this endpoint.

To allow any user to run tests on this endpoint, use the `ALL` parameter, which is the installation default:

```
ALLOW ALL
```

However, the default "**`ALLOW ALL`**" is ***not*** recommended. Although `ALLOW ALL` makes it easy to install an endpoint and see that it's running, it also lets any user who can reach the endpoint potentially use that endpoint as a traffic generator.

To allow only specific users to run tests with this endpoint, remove the `ALLOW ALL` line and identify one or more specific computers by their network addresses. You can specify more than one address per protocol. For example,

```
ALLOW TCP 192.86.77.120
ALLOW TCP 192.86.77.121
```

Specify a connection-oriented protocol (that is, TCP) as the first parameter and provide its corresponding network address as the second parameter. Endpoints listen only for incoming tests on connection-oriented protocols, such as TCP. Datagram tests are set up and results are returned using their "sister" connection-oriented protocol; thus, UDP tests are set up using TCP.

The network address in TCP/IP must be in dotted notation.

Endpoints do not respond to endpoint discovery requests unless the IP address of the computer is specifically allowed (or unless `ALLOW ALL` is specified). This prevents the user of a computer from finding endpoints to which it should not have access.

You cannot use the `ALLOW` parameter to restrict access from one endpoint to another endpoint. The `ALLOW` parameter can be used only to permit (or prevent) access from specific computers to the endpoint at which the parameter is defined.

If, for some reason, you need to restrict your endpoint to access only your own computer, specify your own IP network address rather than `127.0.0.1`. Specifying `127.0.0.1` (the equivalent of `localhost`) allows any other user who specifies `localhost` as Endpoint 1 to access your computer as Endpoint 2.

SECURITY_AUDITING

This keyword determines which access attempts the endpoint keeps track of in its audit file. Here are the possible parameters:

NONE	Writes nothing to the audit file
PASSED	Logs only access attempts that passed the ALLOW address check.
REJECTED	Logs only access attempts that failed the ALLOW address check.
ALL	Logs both passed and rejected access attempts.

If a test initialization fails for a reason other than address checking, no entry is made in the audit file.

AUDIT_FILENAME

This keyword specifies the filespec for the audit file. See "SECURITY_AUDITING" on page 7 to understand the types of events logged in its audit file. The default filename in `endpoint.ini` is `endpoint.aud`. If no drive or path is specified, the audit file uses the drive and path of the endpoint program.

This file contains at most two lines for each endpoint pair that is started on this endpoint. These two lines represent the start of an endpoint instance and the end of that instance.

Each line written to the audit file consists of a set of information about the endpoint instance and what it has been asked to do. The information is written in comma-separated form, so you can load the audit file into a spreadsheet or database. When the audit file is created, an initial header line explains the contents of the subsequent entries.

The following table shows the fields of each entry in the audit file:

Field	Description
Time	The date and time when the entry was created, in the local time zone.
Action	Whether an endpoint instance was "Started" or "Ended."
Endpoint	Whether the endpoint is in the role of Endpoint 1 or Endpoint 2.
Protocol of Console	The network protocol used to contact Endpoint 1.
Network Address of Console	The network address as seen by Endpoint 1. If you encounter problems setting up your `ALLOW` entries, use this value for the protocol address.
Security Result	Whether this `SECURITY_AUDITING` "passed" or was "rejected." If this is an entry for an "Ended" action, this field is reported as "n/a."
Endpoint Partner Protocol	The network protocol used to run the test with a partner endpoint.
Endpoint Partner Address	The network address of a partner endpoint.

ENABLE_PROTOCOL

This keyword lets you control which connection-oriented protocols an endpoint uses to listen for setup connections. This does not affect the network protocols, which can be used to run tests. Here are the possible parameters:

`ALL`

`TCP`

In general, you should use the `ALL` setting (the default). Specify protocols explicitly to reduce the overhead of listening on the other protocols or if you're encountering errors when listening on the other protocols.

See the discussion of the `ALLOW` keyword on page 6 for information about support of the datagram protocols, RTP, and UDP.

Configuring Endpoints for Large-Scale Customization

To customize features such as automatic upgrades, you must edit the `endpoint.ini` file for each endpoint. For obvious reasons, you may not want to undertake such a potentially lengthy procedure. You can extract the files located in `gsendw32.exe` if you need to perform a large-scale customization of endpoint.ini. In addition to WinZip, you'll need the WinZip command-line support add-on and WinZip Self-Extractor. Here's how to use it:

1. Open the file `gsendw32.exe` using WinZip. See "Using WinZip" on page 15 for more information.
2. Extract the files to a temporary directory.
3. Edit or replace the `endpoint.ini` that is now in the temporary directory.
4. Using WinZip, create a new archive that contains all the files in the temporary directory.
5. Using the WinZip Self-Extractor, create a self-extracting executable; for the command line to run, enter the following:

   ```
   SETUP.EXE replace_ini
   ```

Now, anyone who executes the new executable you've created will automatically have the endpoint installed using the `endpoint.ini` file that you've customized.

To create a file that silently self-installs with a custom endpoint.ini:

1. Open the file `gsendw32.exe` using WinZip. See "Using WinZip" on page 15 for more information.
2. Extract the files to a temporary directory.
3. Edit or replace the `endpoint.ini` that is now in the temporary directory.
4. Create a custom response file (say, `customer.iss`); enter

   ```
   i. SETUP -noinst -r -f1.\customer.iss
   ```

5. Using WinZip, create a new archive that contains all the files in the temporary directory.
6. Using the WinZip Self-Extractor, create a self-extracting executable; for the command line to run, enter the following:

   ```
   SETUP.EXE replace_ini -s -f1.\CUSTOMER.ISS
   ```

Now, anyone who executes the file you've created will automatically have the endpoint installed using `customer.iss` as the response file, and the `endpoint.ini` file installed will also be the customized version you created.

Chapter 3

Microsoft Windows Me

This chapter explains the installation, configuration, and operation of the Performance Endpoint software for Microsoft Windows Millennium Edition (Me).

The endpoint software for Windows Me is installed from the same file as the endpoint software for Windows 2000/XP/2003. However, some code, hardware and software requirements, installation instructions, and endpoint capabilities are different for the endpoint actually installed on the Windows Me operating system. See the following topics for details:

See "Microsoft Windows 2000, Windows XP, and Windows Server 2003" on page 77 for information about the endpoint for other Windows operating systems.

Installation Requirements for Windows Me Endpoints

Here's what you need to run the endpoint software with Microsoft Windows Me:

- A computer capable of running Windows Me well. This implies a CPU such as an Intel 80386, 80486, a member of the Pentium family, or equivalent. A Pentium or better is recommended.
- Eight MBytes of random access memory (RAM); 16 MBytes of RAM is recommended.

  The total RAM requirement depends on the RAM usage of the underlying protocol stack and the number of concurrent connection pairs. Since only about 20 connections are possible with a Windows Me endpoint, additional memory is probably not required.

- A hard disk with at least 4 MBytes of space available.
- Microsoft Windows Me with the latest service packs applied. We strongly recommend that you get up-to-date with the latest Windows Me service levels. "Getting the Latest Fixes and Service Updates" on page 23 discusses how to get the latest software.
- One or more compatible network protocol stacks, as described in "Configuration for TCP/IP" on page 19.

Installing the Endpoint for Windows Me

Following are instructions for installing the endpoint from a CD-ROM or from the Web.

- "Installing from a CD-ROM" on page 13
- "Installing from the Web" on page 14
- "Using WinZip" on page 15
- "Unattended Installation for Windows Me" on page 16
- "What Happens During Installation" on page 16

Installing from a CD-ROM

To install the endpoint from a CD-ROM:

1. Put the CD-ROM in your CD-ROM drive.
2. Click **Start > Run**. The Run dialog box is displayed.
3. In the **Open** field, enter the following:
   `[drive:]\Endpoint\Win32\gsendw32.exe`
4. If a previous version of the endpoint is present, you are asked if you want to remove it. Click **OK** if appropriate.
5. The next dialog box lets you select the directory for the endpoint. We recommend installing the endpoint on a local hard disk of the computer you're using (if you install on a LAN drive, the additional network traffic will influence your performance results).

   If you have previously installed endpoints, the default directory is where you previously installed them. If you have not previously installed endpoints but have installed other NetIQ products, the default directory is the same level as the one where your other products are installed. For example, if you installed AppManager, Vivinet Diagnostics, or Vivinet Assessor in `C:\Program Files\NetIQ\[AppManager][VivinetAssessor][VivinetDiagnostics]`, the default directory is `C:\Program Files\NetIQ`. If you have not previously installed other NetIQ products, the default drive is the first drive with enough disk space for the endpoints; the default directory is `\Program Files\NetIQ\Endpoint`.
6. The next dialog box contains two check boxes:
   - The first check box allows you to install pre-built data files. We recommend that you clear this box. This feature is for Chariot users only.
   - Check the second check box to start the endpoint on installation. If you leave the box unchecked, the endpoint is started when you reboot Windows Me.

Installing from the Web

To install an endpoint you've downloaded from the Web:

1. Save the endpoint to a directory on a local hard drive.
2. Use Windows Explorer to navigate to the endpoint file, `gsendw32.exe`, and double-click to unzip it and activate Setup. Refer to "Using WinZip" on page 15 for instructions.

   If a previous version of the endpoint is present, you are asked whether you want to remove it.
3. The next dialog box after the Software License Agreement lets you select the directory for the endpoint. We recommend installing the endpoint on a local hard disk of the computer you're using (if you install on a LAN drive, the additional network traffic will influence your performance results).
4. If you have previously installed these endpoints, the default directory is where you previously installed them. If you have not previously installed endpoints but have installed other NetIQ products, the default directory is the same level as the one where your other products are installed. For example, if you installed AppManager, Vivinet Diagnostics, or Vivinet Assessor in `C:\Program Files\NetIQ\[AppManager][VivinetAssessor][VivinetDiagnostics]`, the default directory is `C:\Program Files\NetIQ`. If you have not previously installed other NetIQ products, the default drive is the first drive with enough disk space for the endpoints; the default directory is `\Program Files\NetIQ\Endpoint`.

   If an endpoint is already installed, you will be prompted to remove the previous installation.
5. The next dialog box contains two check boxes:
   - The first check box allows you to install pre-built data files. We recommend that you clear this box. This feature is for Chariot users only.
   - Check the second check box to start the endpoint on installation. If

you leave the box unchecked, the endpoint is started when you reboot Windows Me.

When you've completed installation, refer to "Configuring Windows Me Endpoints" on page 18 to make sure your endpoint is ready to be used in testing and monitoring.

Using WinZip

If you are installing endpoints on Windows, you first need to unzip the `gsendw32.exe` file from the CD. We recommend using WinZip version 7.0 or higher. Follow these steps to unzip the file:

1. Open the WinZip application.
2. Click **File > Open Archive**. The Open Archive dialog box is displayed.
3. Browse to the `Endpoint\Win32` directory on the endpoint CD-ROM and select the executable endpoint file `gsendw32.exe`.
4. Click **Open** to unzip the files. The files that were unzipped are shown in the Window.
5. Click **Action > Extract**. The Extract dialog box is displayed.
6. Browse to the directory where you want to save the files. This location should be accessible by users who need to install the endpoint.
7. Click **Extract**. The files are extracted to the directory you selected.

Unattended Installation for Windows Me

Unattended installation (also called *silent installation*) is available for the endpoints for Windows. You install an endpoint once, by hand, while the install facility saves your input in an answer file. You can then install that same endpoint silently on other computers, that is, without providing input other than the answer file.

First, run `gsendw32.exe`. An answer file called `update.iss` is created in the `\Updates` subdirectory of the directory where you installed the endpoint.

To perform a silent installation, specify the "`-s`" option on `SETUP`. Make sure the answers documented in the answer file `update.iss` are appropriate for the silent installation. If the `update.iss` file is not in the same directory as `setup.exe`, then specify the path and filename with the "`-f1`" option. For example, here's how to install using the `update.iss` file in the `\Program Files\NetIQ\Endpoint` directory on our `n:` LAN drive:

```
SETUP -s -f1n:\Program Files\NetIQ\Endpoint\update.iss
```

If you don't specify the path and filename with `-f1`, the default filename is `setup.iss`. Don't mix the `.iss` files among different Windows operating systems because their endpoint installations require slightly different input.

It's common to use unattended install from a LAN drive. Be sure you've copied all of the files for each type of endpoint into a single directory (rather than into separate diskette images), and you've created your initial `update.iss` file from that directory. Unattended installation does not keep track of diskette label information, and will need user input if you install from separate disk images. You probably don't want your unattended installation to ask you for `n:\disk1\`, `n:\disk2\`, and so on.

What Happens During Installation

Here's what happens during the installation steps. Let's say you install the endpoint into the directory `\Program Files\NetIQ\Endpoint`. A directory is created with the following contents:

- The executable programs

- The `README` file
- The directory `\Cmpfiles`. This directory contains files with the `.cmp` file extension. These are files containing data of different types, such as typical text or binary data. These files are used by the endpoint as data on `SEND` commands. The different data types can be used to vary the data compression performance of your network hardware and software.
- The file `endpoint.ini`. See "Endpoint Initialization File" on page 5 for information about tailoring this file for individual endpoints.

The installation process for a Windows Me endpoint makes no changes to `CONFIG.SYS` or `AUTOEXEC.BAT`. The installation process does, however, involve adding the endpoint to the Registry so that the endpoint starts automatically when you start a Windows Me computer.

Removing the Endpoint Package

If you need to remove the endpoint package from your hard disk, follow these steps:

1. Click **Start > Settings > Control Panel**.
2. Click the **Add/Remove Programs** icon. The Add/Remove Programs Properties dialog box is displayed.
3. Highlight **NetIQ Endpoint** and click **Add/Remove**. The uninstallation program begins. After the program is completed, the endpoint should be uninstalled.

Removing the Endpoint Manually

If the uninstallation program is unable to uninstall the endpoint, you will need to manually uninstall the endpoint.

For detailed instructions on manually removing the endpoints, see the Performance Endpoints FAQ page in the Knowledge Base on our Web site at www.netiq.com/support/pe/default.asp.

Configuring Windows Me Endpoints

The Performance Endpoint program is a 32-bit application for Windows Me, using network application programming interfaces, such as WinSock, for all of its communications. The endpoint dynamically configures its own programs, so you do not have to update the configuration files for your communications software. However, your communications software must be configured and running correctly. The following steps guide you through this verification.

- Determine the network addresses of the computers to be used in tests
- Verify the network connections

The following topics describe how to accomplish these steps for Windows Me:

- "Configuration for TCP/IP" on page 19
- "Determining the IP Address" on page 19
- "Determining the IP Address" on page 19
- "Testing the TCP Connection" on page 20
- "Sockets Port Number" on page 20

Configuration for TCP/IP

The RTP, TCP, and UDP protocols use TCP/IP software for network communications. TCP/IP offers two forms of network addresses: IP addresses and domain names. An IP address is a 32-bit numeric address. It is represented in dotted notation as a set of four numbers separated by periods, such as `199.72.46.202`. The alternative, domain names are in a format that is easier to recognize and remember, such as www.netiq.com. To use domain names, you need either a Domain Name Server (DNS) set up in your network or an `/etc/hosts` file on each computer.

Determining the IP Address

The easiest way to find the local IP address on a Windows Me computer is to enter the following at a command prompt:

```
WINIPCFG
```

Users of TCP/IP on other operating systems may be familiar with the `NETSTAT` command:

```
NETSTAT -N
```

This shows a line of text for each active connection. The local IP address is in the second column of each row.

You can also find and change your IP address using the graphical user interface. Click **Start > Settings > Control Panel** and double-click the **Network** icon. The installed network components are shown.

Double-click **TCP/IP** to get to the TCP/IP Properties. Select the **IP Address** page to see or change your local IP address. Select the **DNS Configuration** page to see or change your domain name. If the DNS Configuration is empty, avoid using domain names as network addresses. Use numeric IP addresses instead.

Testing the TCP Connection

Ping is a simple utility program, included in all TCP/IP implementations. To check the connection from one computer to another, enter the following at a command prompt:

```
ping xx.xx.xx.xx
```

Replace the x's with the IP address of the target computer. If Ping returns a message that says "`Reply from xx.xx.xx.xx ...`," the Ping worked. If it says "`Request timed out`," the Ping failed, and you have a configuration problem.

Make sure that you can run Ping successfully from the AppManager, Vivinet Assessor, or Vivinet Diagnostics Console to each computer serving as Endpoint 1, and between each pair of endpoints involved in a test, before starting your testing.

Sockets Port Number

TCP/IP applications use their network address to decide which computer to connect to in a network. They use a Sockets port number to decide which application program to connect to within a computer.

The TCP/IP sockets port for endpoints is 10115. This port number is used during the initialization of a test; during the actual running of the test, other port numbers are used.

Running Windows Me Endpoints

The following topics describe starting and stopping the endpoint and configuring the endpoint for IP multicast and QoS support in Windows Me operating systems.

Starting a Windows Me Endpoint

The endpoint is installed as a service, which means there's nothing visible while it's running. During installation the endpoint is configured to automatically start when the system reboots. This causes `endpoint.exe` to be started automatically when Windows Me is started.

If you stop `endpoint.exe` and need to restart it without restarting Windows Me, enter

```
ENDPOINT
```

at a command prompt (from the directory where you installed our software).

A single running copy of `endpoint.exe` handles all concurrent tests. If the endpoint program is already running and you try to start another copy, you see a popup error dialog box, "`Endpoint is already running.`"

Stopping a Windows Me Endpoint

To stop the endpoint program, use the command-line option `-k`. Invoke this command from the directory where you've installed the endpoint:

```
endpoint -k
```

Disabling Automatic Startup

To prevent the endpoint from running automatically at startup, take the following steps:

1. Open the Registry edit utility using the command `REGEDIT`.
2. Navigate to `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows \CurrentVersion\RunServices` and open it.
3. Write down the value for the variable **NetIQ Performance Endpoint**, so that you can restart the endpoint as a service later. Delete the **NetIQ Performance Endpoint** key from the Registry.

If you want to restore the setting later, you must do so manually.

Disabling Your Screen Saver

Screen savers can significantly lower the throughput that's measured by an endpoint. We recommend disabling your screen saver at endpoint computers while running tests.

Disabling the Suspend Program

The Suspend program is a power management program. If you run a test to an endpoint with Suspend enabled, it will not complete. Disabling the Suspend program should eliminate this problem.

Logging and Messages

Although most error messages encountered by an endpoint are returned to the AppManager, Vivinet Assessor, or Vivinet Diagnostics Console, some may be logged to disk. Errors are saved in a file named `endpoint.log`, in the directory where you installed our software. To view an error log, use `FMTLOG`. The version of `FMTLOG` shipped with the Windows Me endpoint runs as a command from a command prompt. `FMTLOG` reads from a binary log file, and writes its formatted output to `stdout`. Use the following `FMTLOG` command:

```
FMTLOG log_filename > output_file
```

For example, to format the error log and write the formatted output to a file named `log.txt`, enter the following at a command prompt:

```
FMTLOG d:\Program Files\NetIQ\endpoint\endpoint.log >log.txt
```

In addition, the endpoint code does a lot of internal checking on itself. Our software captures details related to the problem in an ASCII text file named `assert.err` in the directory where you installed the endpoint. Save a copy of the file and send it to us via email for problem determination.

Getting the Latest Fixes and Service Updates

We've found that communications software is often fragile. Its developers are constantly working to make it more robust, as the software gets used in an ever-wider set of situations. We therefore recommend working with the very latest software for the underlying operating system and communications software. The following is one of the best sources we've found for the Windows Me software used by the endpoint program.

Microsoft posts code and driver updates directly to the following Web site: www.microsoft.com/windows/downloads/

Index

U

W