NetIQ Performance Endpoints 5.1

User Guide

October 2017

Legal Notice

Contents

About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

User Guide for AppManager Control Center

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

Administrator Guide for AppManager

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

Upgrade and Migration Guide for AppManager

Provides complete information about how to upgrade from a previous version of AppManager.

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The AppManager library is available in Adobe Acrobat (PDF) format from the AppManager Documentation page of the NetIQ Web site.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

1 Introducing Performance Endpoints

This guide contains information about installing, configuring, and running NetIQ Performance Endpoints. Performance Endpoints are lightweight software agents that allow you to send synthetic VoIP traffic between two nodes on your network and take performance measurements.

Endpoints are available for several operating systems. The latest version of the endpoint software can be downloaded free from the Web. A single installation file for each supported operating system is available at the Current Performance Endpoints Product Upgrades page.

You cannot run endpoint software from removable media, such as CD-ROM/DVD. You must install it on a computer.

The following table identifies the NetIQ products that support Performance Endpoints. System requirements for individual endpoint packages are itemized in the corresponding chapters in this guide.

NetIQ Product	Vivinet Assessor	Vivinet Diagnostics	AppManager ResponseTime for Networks	AppManager for VoIP Quality
Endpoint				
Microsoft Windows	Yes	Yes	Yes	Yes
NOTE: Older versions of Endpoint exist for the following platforms				
HP-UX	No	No	Yes	No
IBM AIX	No	No	Yes	No
Linux for Cobalt RaQ3 (x86)	Yes	Yes	Yes	Yes
Linux x86 (TAR)	Yes	Yes	Yes	Yes
Linux x86 (RPM)	Yes	Yes	Yes	Yes
Microsoft Windows (Web-based)	Yes	No	No	No
Sun Solaris (SPARC and x86)	Yes	Yes	Yes	Yes

2 Endpoint Initialization File

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

- Restrict the use of this endpoint to specific AppManager, Vivinet Diagnostics, or Vivinet Assessor consoles
- 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 supported operating systems.

By default, the endpoint initialization file contains the following keywords and parameters. You can change these keywords and parameters to tailor individual endpoints for your needs.

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

The `endpoint.ini` file is an editable text file. There is a separate copy for each operating system. You should customize it before endpoint installation. Your changes are then incorporated into each installation 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 installation from that drive.

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, although `ALLOW ALL` is the default, it is *not* recommended. `ALLOW ALL` makes it easy to install an endpoint and see that it is running, but 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.

To restrict your endpoint to access only your own computer, specify your own IP network address rather than `127.0.0.1`. Specify `127.0.0.1`, the equivalent of `localhost`, to allow another user who specifies `localhost` as Endpoint 1 to access your computer as Endpoint 2.

SECURITY_AUDITING

This keyword determines which access attempts the endpoint logs in its audit file. The following table identifies 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. For more information, see “SECURITY_AUDITING” on page 12. The default filename is `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."

Field	Description
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. There are two possible parameters:

```
ALL
TCP
```

In general, you should use the `ALL` setting, which is the default. Specify protocols explicitly to reduce the overhead of listening on the other protocols or if you encounter errors when listening on the other protocols.

For more information, see “ALLOW” on page 11.

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 manually undertake such a potentially lengthy procedure. To perform a large-scale customization of `endpoint.ini`, you can extract the files contained in `gsendw32.exe`, which is installed by default in when you install the Performance Endpoint software. In addition to WinZip, you need the WinZip command-line support add-on and WinZip Self-Extractor.

To extract the files in gsendw32.exe:

1. From the location in which you installed the Performance Endpoint software, double-click the `gsendw32.exe` file and extract the files to a temporary directory.
2. Edit or replace the `endpoint.ini` that is now in the temporary directory.
3. Using WinZip, create a new archive that contains all the files in the temporary directory.
4. Using the WinZip Self-Extractor, create a self-extracting executable. To enable the command line to run, enter the following:

   ```
   SETUP.EXE replace_ini
   ```

Now, anyone who runs the executable you created will automatically have the endpoint installed using the `endpoint.ini` file you customized.

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

1. Double-click the `gsendw32.exe` file and extract the files to a temporary directory.
2. Edit or replace the `endpoint.ini` that is now in the temporary directory.
3. Create a custom response file, such as `customer.iss`. For example, enter

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

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 -s -f1.\CUSTOMER.ISS
   ```

Now, anyone who runs the file you created will automatically have the endpoint installed using `customer.iss` as the response file, and the `endpoint.ini` file that is installed will be the customized version you created.

3 Microsoft Windows

This chapter explains the installation, configuration, and operation of the Performance Endpoint software for Microsoft Windows.

The following NetIQ products support endpoints installed on all supported Windows platforms:

- AppManager ResponseTime for Networks module
- AppManager for VoIP Quality module
- Vivinet Assessor
- Vivinet Diagnostics

System Requirements

The computer on which you want to install the endpoint for Microsoft Windows must meet the following requirements:

Requirement	Notes
Microsoft Windows operating system	One of the following, with the latest service packs installed: ◆ Windows Server 2016 ◆ Windows 10 (32-bit or 64-bit) ◆ Windows Server 2012 R2 ◆ Windows 8.1 (32-bit or 64-bit) ◆ Windows Server 2012 ◆ Windows 8 (32-bit or 64-bit) ◆ Windows Server 2008 R2 ◆ Windows 7 (32-bit or 64-bit) ◆ Windows Vista (32-bit or 64-bit) **For IP Quality of Service (QoS)**: ◆ For Windows 7 or later client operating systems, or Windows Server 2008 R2 or later server operating systems require the Quality Windows Audio Video Experience (qWAVE) feature. For more information, see “Installing qWAVE to Monitor QoS Settings” on page 16. ◆ Windows Vista and Windows Server 2008 (non-R2) do not support setting DSCP bits. **NOTE:** To allow VoIP RTP traffic to run on dynamic ports, you must disable the Windows firewall on any computer on which Performance Endpoint software is running.

Requirement	Notes
Compatible network protocol software for RTP, TCP, and UDP	TCP/IP software is provided as part of the network support with all supported versions of Windows. Quality of Service (QoS) support for TCP/IP is available in all supported versions of Windows that support QoS, except for Windows Vista and Windows Server 2008 (non-R2).

Installing qWAVE to Monitor QoS Settings

For the endpoint to properly monitor QoS settings on a computer running Windows Server 2008 R2 or later server operating systems, you need to install the Quality Windows Audio Video Experience (qWAVE) feature, and the associated service must be running.

The qWAVE feature is enabled by default on computers running Windows 7 and later client operating systems.

To install qWAVE:

1. Launch the Windows Server Manager.

   NOTE: You can also install qWAVE by running the following at a command prompt:

   ```
   servermanagercmd -install qwave
   ```

2. Select **Features** in the tree on the left, and then select **Add Features** in the right-hand pane.
3. From the feature list, select **Quality Windows Audio Video Experience**.
4. Click **Next**, and then click **Install**.
5. After the qWAVE installation completes, reboot the server.

Enabling QoS for a Windows Server 2003 or Windows XP Computer

To enable QoS settings on endpoints running Windows Server 2003 or Windows XP, you must add the DisableUserTOSSetting `DWORD` registry value to each endpoint computer. Add the following `DWORD` registry value at the endpoints:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableUserTOSSetting = 0
```

Reboot the endpoint computers after you edit the registry settings.

NOTE: Windows Server 2008 R2 and Windows 7 do not require the DisableUserTOSSetting registry value.

Installing Endpoint

Ensure your networking software is working correctly before installing the endpoint software. For more information, see the Help for your networking software, and “Configuring Windows Endpoints” on page 19.

The endpoint for Microsoft Windows is installed as a service and runs as a service. To successfully install the endpoint, you must be logged in with Administrator authority. The permissions of the directory where the endpoint is installed must also be set to allow the account running the endpoint service full control permission on all files in the `NetIQ\Endpoint` directory or the directory where you installed the endpoint, plus any relevant subdirectories.

The security implementation in Windows Server 2003 differs noticeably from that in earlier versions of Windows. Before you install the endpoint on Windows Server 2003, ensure your user account is running in “Install” mode and not in “Execute” mode.

To change the mode so you have the necessary installation privileges, run the following at a command prompt:

```
change user /install
```

If you try to install from the wrong mode, the installation on Windows Server 2003 fails with the following message: `The InstallShield-generated file that allows uninstallation is missing`.

Installing from the Web

To install endpoint:

1. Save the endpoint download package to a directory on a local hard drive.
2. Navigate to the endpoint file, `gsendw32.exe`, and double-click it to begin installation.
3. The first dialog box after the Setup dialog box lets you select the directory where the endpoint will be installed. You should install it on a local hard disk of the computer you are using. If you install on a LAN drive, the additional network traffic may influence your performance results. The default directory is `\Program Files\NetIQ\Endpoint`, on your boot drive.
4. If you have a previous installation of the endpoint, you will be asked if you want it removed. If you click **Yes**, the previous installation is removed, and the new installation continues. If you click **No**, the install program exits with no changes to your existing installation because a new version cannot be added until the old version is removed. It then adds Endpoint (the endpoint program) as a service.
5. The next dialog box contains two check boxes.
   - The first check box lets you opt to install pre-built data files. You should clear this box. This feature is for Chariot users only.
   - Check the second box to start the endpoint installation. If you leave this box cleared, the endpoint starts when you restart the computer. No window is shown while the endpoint is running because it runs as a service.

Windows services are controlled from the Services dialog box inside the Control Panel. To restart a service without restarting Windows, use the Services dialog box.

You can also manually start the endpoint after installation. For more information, see “Starting Endpoint” on page 20.

To prevent the endpoint from running automatically on startup, see the section titled “Disabling Automatic Startup” on page 22. You can manually restore the setting.

After you complete installation, see “Configuring Windows Endpoints” on page 19 to ensure your endpoint is ready for testing and monitoring.

Unattended Installation

Unattended, or *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.

To perform silent installation:

1. Run `gsendw32.exe`. An answer file called `update.iss` is created in the `\Updates` subdirectory of the directory where you installed the endpoint.
2. Specify the “`-s`” option on `SETUP`. Ensure the answers documented in the answer file `update.iss` are appropriate for the silent installation.
3. If the `update.iss` file is not in the same directory as `setup.exe`, specify the path and filename with the “`-f1`” option. The following example shows how to install using the `update.iss` file in the `\Program Files\NetIQ\Endpoint` directory on a NetIQ `n:` LAN drive:

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

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

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

What Happens During Installation

During installation, the endpoint is installed by default into the `\Program Files\NetIQ\Endpoint` directory. The directory is created with the following contents:

- The executable programs
- 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 `endpoint.ini` file. For more information, see Chapter 2, “Endpoint Initialization File,” on page 11.

The endpoint is installed as a service, which means nothing is visible while the endpoint is running. During installation, the endpoint is configured to automatically start when the system reboots. A service can be controlled from the Services dialog box inside the Control Panel. For more information, see “Starting Endpoint” on page 20.

Removing Endpoint Software

You can use the **Add or Remove Programs** or **Programs and Features** option from the Control Panel to uninstall the endpoint software.

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

Configuring Windows Endpoints

The endpoint program uses network application programming interfaces, such as Sockets, 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 process.

1. Determine the network addresses of the computers to be used in tests.
2. Select a service quality.
3. Verify the network connections.

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, such as `199.72.46.202`. As an alternative, use domain names, which are in a format that is easier to recognize and remember. 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

To determine the local IP address for a Windows computer, enter the following at a command prompt:

```
IPCONFIG
```

If your TCP/IP stack is configured correctly, your output will look like the following:

```
Windows IP Configuration
Ethernet adapter Local Area Connection:
IP Address. . . . . . . . . . : 10.10.44.3
Subnet Mask . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . : 10.10.44.254
```

The local IP address is shown in the first row. In this example, it is `10.10.44.3`.

To determine a the local hostname for a Windows computer, enter the following at a command prompt:

```
HOSTNAME
```

The current hostname is shown in the first row.

Testing the TCP/IP 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.

From your AppManager, Vivinet Assessor, or Vivinet Diagnostics console computers, ensure you can run Ping successfully to each computer serving as Endpoint 1, and between each pair of endpoints involved in a test, before starting your testing with TCP/IP.

Starting Endpoint

By default, the endpoint service is configured to start automatically, which means you will not see a window for the program when it is running. Because the endpoint runs as a service, you do not have to be logged into your computer for the endpoint to run.

Only a user ID with Administrator authority is permitted to start or stop Windows services.

If you stop the endpoint service, you can restart it without restarting Windows. Use one of the following methods to restart the endpoint service:

- At a command prompt, enter `net start netiqendpoint`
- In the Services dialog box, select **NetIQ Endpoint** and click **Start** (or **Play**). For example, to restart `endpoint.exe` in Windows XP, navigate to the Services dialog box, right-click **NetIQ Endpoint**, and select **Restart**. The status changes to "started" when the service is successfully started.

NOTE: A single running copy of the endpoint service handles one or more concurrent tests.

Stopping Endpoint

Only a user ID with Administrator authority is permitted to start or stop Windows services.

Use one of the following methods to stop the endpoint service:

- At a command prompt, enter the following:

  ```
  net stop netiqendpoint
  ```

- In the Services dialog box, right-click **NetIQ Endpoint** and select **Stop**. The status is blank when the endpoint program has stopped.

Disabling Your Screen Saver

Screen savers can significantly lower the throughput measured by an endpoint. You should disable your screen saver at endpoint computers while running tests, Diagnoses, or Assessments.

Using the SetAddr Utility

This topic is applicable only for endpoints used with NetIQ AppManager.

Endpoints for Windows operating systems ship with a utility that helps you quickly create virtual IP addresses on Windows endpoint computers. Virtual addresses are useful when you are testing hundreds or even thousands of endpoint pairs using only a few computers as endpoints. To all intents and purposes, the traffic on the network is identical, whether you are using “real” or virtual addresses.

When you install a Windows endpoint, `Setaddr.exe` for 32-bit Windows is automatically installed in the same directory. For 64-bit Windows, a 64-bit version of `Setaddr.exe` is installed. The two versions of `SetAddr` cannot be used across operating systems with different architectures.

The usage is as follows:

```
setaddr [-dr] -a N -f Addr -t Addr -i Addr -s Addr
| -l[a]
| -da
| -ds -f Addr -s Addr
```

where “`N`” indicates the adapter number of the NIC card you are assigning virtual addresses to, and “`Addr`” indicates the virtual addresses or subnet mask you are assigning to it.

Options:

```
-l     List all network adapters
-la    List all network adapters and their IP addresses
-a     Adapter to modify (number given by -l options)
-dr    Delete a range of addresses
-da    Delete all addresses
-ds    Delete a single address
-f     From address
-t     To address
-i     Increment by
-s     Subnet Mask
```

The `-d` flags cannot be used to delete a computer’s primary IP address.

The `-i` flag lets you determine how the range of addresses will be created. This is an optional field. By default, `SetAddr` increments the range by one in the final byte only. This “increment by” value is represented as “`0.0.0.1`”. Enter a value (0-255) for each byte of the 4-byte IP address. A value of 1 specifies that the address values in that byte will be incremented by one when `SetAddr` creates the range. For example, enter

```
setaddr -f 10.40.1.1 -t 10.40.4.250 -i 0.0.1.1 -s 255.255.0.0
```

SetAddr creates 1000 virtual addresses.

Known Limitations:

- IPv4 only.
- `SetAddr` only works on computers with fixed IP addresses. DHCP-enabled adapters cannot be used.
- Before testing, restart the computer that has the NIC to which you assigned virtual IP addresses. `SetAddr` modifies some Windows Registry keys, and restarting is required for the changes to take effect.
- The number of virtual addresses you can assign to a single adapter depends on the protocol stack and the size of the Windows Registry. NetIQ benchmarked measurements using computers running up to 2500 virtual addresses, which is a recommended limit.

- No checking is done to ensure that thousands of addresses are not being created. More TCP/IP stack resources are required to manage virtual addresses.
- You may only add Class A, B, and C virtual IP addresses. Loopback addresses and Class D and E IP addresses are invalid. Valid address ranges, then, are `1.x.x.x` to `233.x.x.x`, excluding `127.x.x.x`.
- When more than 2250 virtual address are defined on Windows 2000 computers, all the LAN adaptor icons disappear from the Network and Dial-up Connections dialog box in My Network Places. You can still see the adaptors by invoking `ipconfig` or setaddr from the command line, and the addresses are still reachable. Removing some virtual addresses so that fewer than 2250 were specified and restarting the computer solved the problem.

Disabling Automatic Startup

To disable the automatic starting of the endpoint:

1. Navigate to the Services dialog box and then double-click **NetIQ Endpoint**.
2. In the **Startup type** field, select **Manual**.
3. Click **OK** to save the new setting and exit the dialog box. The endpoint will no longer start automatically when you restart the computer. However, you can manually start the endpoint.

How to Tell Whether a Windows Endpoint Is Active

The **Status** field in the Services dialog box shows whether the NetIQ Endpoint service has started.

You can also use the Windows Performance Monitor program to look at various aspects of the endpoint. Start Performance Monitor by double-clicking its icon in the **Administrative Tools** group. Click **Edit > Add to Chart**. Select the **Process** object and the **Endpoint** instance. Then add the counters you are interested in, such as thread count or % of processor time. In the Steady state (that is, no tests are active), Thread Count will show about six threads active for the endpoint. The exact number depends on the number of protocols in use.

Logging and Messages

Most error messages encountered on an endpoint are returned to the AppManager, Vivinet Assessor, or Vivinet Diagnostics console computer. However, some may be logged to disk. Errors are saved in a file named `ENDPOINT.LOG`, in the directory where you installed the endpoint. To view an error log, use the command-line program named `FMTLOG.EXE`. The program `FMTLOG.EXE` reads from a binary log file, and writes its formatted output to `stdout`. Use the following `FMTLOG` command:

```
FMTLOG log_filename > output_file
```

The endpoint performs extensive internal cross-checking to catch unexpected conditions early. If an assertion failure occurs, the file `assert.err` is written to the directory where you installed the endpoint.