Performance Endpoints 5.1

Web-Based

April 2006

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 1995-2006 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, Provider-1, SiteManager-1, and VPN-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, AppAnalyzer, AppManager, ConfigurationManager, the cube logo design, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Knowing is Everything, Knowledge Scripts, MailMarshal, Marshal, Mission Critical Software for E-Business, MP3check, NetConnect, NetIQ, the NetIQ logo, NetIQ Change Guardian, NetIQ Firecall Administrator, NetIQ Firewall Suite, NetIQ Group Policy Administrator, NetIQ Group Policy Guardian, the NetIQ Partner Network design, Patch Manager, NetIQ Security Analyzer, NetIQ Security Manager, NetIQ Security Reporting Center, NetIQ Vulnerability Manager, WebMarshal, PSAudit, PSDetect, PSPasswordManager, PSSecure, RecoveryManager, Server Consolidator, SQLcheck, VigilEnt, Vivinet, Work Smarter, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Contents

About This Guide

Intended Audience iii

Using This Guide iii

Conventions Used in this Guide iv

Complementary NetIQ Products iv

Contacting NetIQ v

Chapter 1 **Introduction to Performance Endpoints**

Operating System and Protocol Stack Support 2

Endpoint Capabilities 2

Chapter 2 **Endpoint Initialization File**

ALLOW. 6

SECURITY_AUDITING 7

AUDIT_FILENAME. 7

ENABLE_PROTOCOL 8

Configuring Endpoints for Large-Scale Customization. . . 9

Chapter 3 **Web-Based Performance Endpoint**

Running the Web-Based Endpoint 12

Error Handling 13

Compatibility with Other Endpoints 13

Stopping the Web-Based Endpoint 14

Index

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, "Web-Based Performance Endpoint," explains the installation and operation of the Web-Based Performance Endpoint software.

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

Web-Based Performance Endpoint

NetIQ Performance Endpoints are lightweight software agents that allow for testing and monitoring of computers and computer networks. Endpoints are available for several operating systems and are continually updated to support new features in NetIQ AppManager and Vivinet Assessor.

Unlike the endpoints for all of the other supported platforms, the Web-Based Performance Endpoint was not designed to be installed on a computer. Users of the Web-Based endpoint can either run it from the World Wide Web or save it to a local hard disk, but as soon as they restart, or log out of, the computer where it is running, the endpoint stops running.

The Web-Based endpoint runs on the following operating systems:

- Windows Me
- Windows 2000
- Windows XP (32-bit version only)
- Windows Server 2003

Although endpoints for other operating systems still run as long as the computer where they're installed is powered on, the Web-Based endpoint stops running as soon as the user logs out or restarts. Nothing has been written to the Windows Registry on the computer where it ran.

Running the Web-Based Endpoint

To run the Web-Based endpoint on your local computer, use the Web browser on that computer to navigate to **www.netiq.com/download/endpoints**. Click the link labeled **Web-Based Endpoint**.

Unless you are using a utility such as RealDownload to download files from the Web, you are then asked whether you want to run the software from its present location or save it to disk. Click to select one of these options.

Run from Location:

If the download is successful, you'll see a message stating that the endpoint has been started. Click **OK** to close the message.

There's nothing else you need to do. The endpoint is ready for monitoring with AppManager and for VoIP Readiness Assessments with Vivinet Assessor.

Save to Disk:

If you want to save it to disk, save it to the folder where you save your temporary files, such as Temp.

Navigate to the folder where you've saved the endpoint. Double-click the file **endpoint.exe** to start the endpoint. You'll see a message stating that the endpoint has been started. Click **OK** to close the message.

After you start the endpoint, there's nothing else you need to do. The endpoint is ready for monitoring with AppManager and for VoIP Readiness Assessments with Vivinet Assessor.

Note When you save the endpoint to a local hard disk, it makes no difference where you save it. When you restart the computer, a copy of the executable `endpoint.exe` will still be on your hard drive, but it will no longer run until you restart it. Restart the executable by double-clicking it in Windows Explorer.

Error Handling

Unlike endpoints for other operating systems, the Web-Based endpoint doesn't log the errors it encounters. However, it does report errors to the AppManager or Vivinet Assessor Console.

In the case of a connection failure or other failure during testing, the endpoint vanishes silently. The Console will notify you that it can no longer reach the endpoint. You should return to the Web and re-enable the endpoint in the case of such a failure.

Compatibility with Other Endpoints

The Web-Based endpoint cannot run on a computer where another endpoint is already running. For example, you cannot run the Web-Based endpoint on a computer where you have the endpoint for Windows 2000/XP/2003 installed and running. When you attempt to download it, you'll receive an error message.

Correspondingly, if the Web-Based endpoint is running on a computer, you can install one of the conventional endpoints on that computer, but the conventional endpoint will not start running automatically once the installation completes. If the Web-Based endpoint executable is running, you must either stop it before installing another endpoint, or else restart the computer after you complete the installation. The new endpoint will then start running automatically (and the Web-Based endpoint will no longer be present).

Stopping the Web-Based Endpoint

The Web-Based endpoint stops automatically as soon as you restart your computer or log out. However, you can also stop the endpoint manually.

To stop the Web-Based endpoint:

1. Click [`Ctrl+Alt+Delete`] to access Windows Task Manager.
2. Click the **Processes** tab. In Windows Me, you'll already see the list of processes.
3. Highlight the **endpoint.exe** process. Click **End Process** to stop the endpoint and remove it from your computer.

Index

A
ALLOW 6
AUDIT_FILENAME 7

C
conventions, documentation iv

D
documentation, conventions iv

E
ENABLE_PROTOCOL 8
endpoint
    capabilities 2
    initialization file 5
endpoint.aud
    description 7
endpoint.ini
    ALLOW 6
    AUDIT_FILENAME 7
    ENABLE_PROTOCOL 8
    keywords 5
    SECURITY_AUDITING 7

G
gsendw32.exe 9

K
keyword
    ALLOW 6
    AUDIT_FILENAME 7
    ENABLE_PROTOCOL 8
    SECURITY_AUDITING 7

P
protocol support 2

S
SECURITY_AUDITING 7
software requirements 2

W
Web-Based endpoint
    and other endpoints 13
    errors 13
    installing 12
    runnning 12
    stopping 14
    supported platforms 11