EFT143 NetEx/eFT™

for Windows NT™ and Windows 2000™ x86 Systems

Release 5.3.0 N2

Memo To Users

April 6, 2004

6420 Sycamore Lane N #300
Maple Grove, MN 55369

Preface

Proprietary Information Statement

The information in this document is confidential and proprietary to Network Executive Software and may by used only under the terms of the product license or nondisclosure agreement. The information is this document, including any associated software program, may not be disclosed, disseminated, or distributed in any manner without the written consent of Network Executive Software.

Limitations on Warranties and Liability

This document neither extends nor creates warranties or any nature, expressed in implied. Network Executive Software cannot accept any responsibility for your use of the information in this document or for your use of any associated software program. You are responsible for backing up your data. You should be careful to ensure that your use of the information complies with all applicable laws, rules, and regulations of the jurisdictions in which it is used.

Warning: No part or portion of this document may be reproduced in any manner or in any form without the written permission of Network Executive Software.

Restricted Rights

Trademarks

Network Executive Software is a registered trademark of Network Executive Software, Inc.

Windows NT and Windows 2000 are registered trademarks of Microsoft Corporation.

Other product names mentioned in this manual may be trademarks. They are used for identification purposes only.

Support

Customers can contact NESi customer support to request assistance with this software via the following methods:

- By calling 800-854-0359
- By e-mailing support@netex.com
- By filling out a form on the Customer Support page at http://www.netex.com.

Information in this publication is subject to change. Comments concerning the contents of this document should be directed to:

Network Executive Software, Inc.
6420 Sycamore Lane, Suite 300
Maple Grove, MN
Attn: Customer Support

Contents

Introduction

This guide describes how to install the Network Executive Software EFT143 Windows NT and Windows 2000 NetEx/eFT product.

This product has been tested on the following configurations running on Intel x86 processors. Versions of NT before 4.0 are not supported.

- Windows NT Workstation Operating System (OS) version 4.0 Service Pack 6.
- Windows NT Server Network Operating System (NOS) version 4.00 Service Pack 5.
- Windows 2000 Professional SP3.

NetEx/eFT is designed to run over TCP/IP and NetEx/IP (the desired network protocol is selected during product installation). EFT143 N2 for Windows NT and Windows 2000 NetEx/eFT supports TCP/IP and UDP products developed to the Microsoft Windows Sockets Specification version 2, a standard Windows API to a Berkeley Sockets interface. Although many TCP/IP products advertise support for Windows Sockets, not all run full sockets applications without upgrades or patches. Therefore NetEx/eFT will support only TCP/IP products that have been certified with EFT143 N2 Windows NT and Windows 2000 NetEx/eFT. Currently, NetEx/eFT supports the following TCP/IP product:

- Microsoft Windows Sockets version 2, which ships with Window NT and Windows 2000. NetEx/eFT uses the WSOCK32.DLL library that expects exclusively 32-bit arguments.

The NetEx/eFT modules installed will run as Windows NT/Win2K 32-bit applications. The NETEX-eFT client and SI Log programs run as WIN32 applications. The NETEX-eFT Responder, NETEX-eFT Service Initiator, and NETEX-eFT client run as Windows NT/Win2K 32-bit console (text) applications. The NETEX-eFT Service Initiator will be initiated by an NT/Win2K Service called the NETEX-eFT <NET> Service Initiator Service, "eFTSvcInit<NET>" (see "Appendix B. Internal Functions" on page 12 for more information on the Service Initiator modules).

Note: Since EFT143 supports the use of both TCP/IP and NetEx/IP network protocols, the convention throughout this document uses <NET> to indicate either TCP or NTX as selected during product installation.

Prerequisites

- Customers must obtain a software KEY from NESi prior to running the EFT143 software. Customers must contact NESi customer support by e-mail with the customer site name, output from genMAC program (see Appendix F), and the EFT product designator (e.g., EFT143). NESi customer support will supply the necessary key once this information has been received. The customer needs to place this key into the NESikeys file as discussed in Appendix E.
- For EFT143 to run with the NetEx/IP protocol, H140IP must be fully installed, tested, and running.

Service Notes

The following describes current problems and/or limitations with this release of EFT143 NetEx/eFT:

- Starting the Service Initiator as a desktop application (not running as a service) does not generate a warning at startup that the Service Initiator may not be able to authenticate users. Additional privileges are required to run the Service Initiator on the desktop with security enabled. See "Service Initiator" in "Appendix B. Internal Functions" on page 12 for more information on running the Service Initiator on the Desktop.
- The unInstallShield process cannot delete the NETEX-eFT Service Initiator Service if it is running. If an unInstallShield is completed while the NETEX-eFT Service Initiator Service is running, the file SVCINIT.EXE and SVCISERV.EXE will be scheduled to be deleted during the next system boot. If you install a new version of NetEx/eFT prior to the next boot, the new SVCINIT.EXE and SVCISERV.EXE files will be deleted. You should delete the NETEX-eFT Service Initiator Service (using the "NETEX-eFT Delete Service" icon) prior to doing an unInstallShield.
- Remote NetEx/eFT users who specify an encrypted password in the CONNECT command to NetEx/eFT on NT/Win2K should be aware that a case sensitivity issue exists when specifying a local NT/Win2K user name that is optionally requested by the NetEx/eFT ENCRYPT function ("*2" password encryption). The case sensitivity issue does not exist when using a "*1" encrypted password, i.e., a password that has been encrypted without specifying the optional username.

Installation Notes

This section provides complete installation procedures for the EFT143 Windows NT and Windows 2000 NetEx/eFT product.

Before You Begin

Before you begin installation, note the following:

1. Make certain that you have all of the items listed in "Prerequisites" in the "Introduction" section.
2. Add the encrypted Software Key obtained from Network Executive Software to the NESi License Key file (NESikeys.ini) that will normally reside in the SystemRoot directory (normally C:\Winnt). See Appendix E for the format of this file if you need to create it for the first time.
3. If you have previously installed NetEx/eFT on your NT or 2000 system and are ready to install a new release, terminate any currently running NetEx/eFT processes prior to installing a new distribution.

   - Terminate the NETEX-eFT <NET> Service Initiator service. The NETEX-eFT <NET> Service Initiator service, eFTSvcInit<NET>, starts automatically each time the Operating System is initialized. Use the "NETEX-eFT <NET> Delete Service" icon in the Netex folder to stop the "NETEX-eFT <NET> Service Initiator service."

     Other methods that may be used to stop the Service Initiator include:

     Windows NT - Go to Start menu, Settings, Control Panel, Services tab, locate the NETEX-eFT <NET> Service Initiator and verify that the status is blank. If the status is "Started", highlight the service and click the "STOP" button. Wait for the status to indicate the service is stopped.

     Windows 2000 - Go to Start menu, Settings, Control Panel. Click on the Administrative Tools icon, then the Services icon. Locate the "NETEX-eFT <NET> Service Initiator" service and verify that the status is blank. If the status is "Started", right click and select "Stop" from the menu, and then wait for the status to clear.

     or:

     In the *C:\SICOMNT*\SI directory, where *C:\SICOMNT* is the NetEx/eFT install directory, enter:

     ```
     C:\SICOMNT\SI\Setup delete
     ```

     or:

     Go to the Start Menu and select Programs->Netex and double-click NETEX-eFT <NET> Client. At the client prompt, enter the following NETEX-eFT connect command:

     ```
     connect hostname -!control stop
     ```

4. Verify that all NETEX-eFT Responders have completed execution by bringing up "Task Manager" and waiting for all NetEx/eFT applications, if any, to complete.

   Note: When the Service Initiator is running, two associated image names displayed by Task Manager are: "Svciserv<NET>.exe and "SvcInit<NET>.exe".

Step 1. Install the Distribution

Note: We recommend that you uninstall the previous NetEx/eFT software before proceeding with installation. See "To Uninstall NetEx/eFT" on page 9.

Insert the NetEx/eFT installation disk into your Windows NT/Win2K machine.

This version of NetEx/eFT requires 1 MB of disk space. The NetEx/eFT distribution may be easily loaded onto any Windows NT/Win2K Workstation or Windows NT/Win2K Server.

To start the NetEx/eFT installation on Windows NT or Windows 2000 requires the following steps:

1. Select the "Add/Remove Programs" Applet from the Windows NT/Win2K Control Panel. Click the "Install" button. Click "next:" and the Applet will find the "Setup" application on the floppy drive. Click "Finish" to start the install.
2. Select the destination directory and folder.
3. The install program will then enable you to select the network protocol (NETEX/IP, the default, or TCP/IP). After making the selection, click Next to continue.
4. The install program will then prompt that it is creating a NETEX Folder, copying the files, and adding icons to the NETEX Folder.
5. The NETEX Folder will include the following icons:
    - **NETEX-eFT <NET> Client** - Initiates the NETEX-eFT <NET> Client program.
    - **NETEX-eFT <NET> SI Log** - Allows users to view the Service Initiator log file.
    - **NETEX-eFT <NET> Delete Service** - Deletes the NETEX-eFT <NET> Service Initiator service. It simply runs the "\SICOMNT\SI\Setup delete" command.

Step 2. Verify that the Service Initiator is Started

Note: You should shut down and restart your NT/Win2K machine before proceeding.

NetEx/eFT Setup will install and start an NT/Win2K Service called the NETEX-eFT <NET>Service Initiator. To verify that the service is running, start the "NETEX-eFT <NET> SI Log" application and verify that the line "Service Offered" is at the end of the log. If this line is not present, check the Log for an error message that may indicate why this service failed to start. For example, the following message will indicate that a valid encrypted Software Key for the current release of EFT143 does not exist in the NESi License Key file:

```
ntx license: Product 'EFT143' not licensed to run on this platform
```

By default, the Service Initiator Service will start each time the system is started/restarted. For more information on this service, see **Appendix B: Internal Functions.**

To Uninstall NetEx/eFT

1. Make certain you have completed all of the items in the section "Before You Begin".
2. Terminate the NETEX-eFT <NET> Service Initiator and the NETEX-eFT <NET> Client.
3. Use the "Add/Remove Programs" Applet from the Windows NT/Win2K Control Panel.
4. Highlight NETEX-eFT<NET> and click on Add/Remove.

Update Summary

Version 5.3.0 N2

The following features or corrections are included:

- Corrected customer reported issue where eFT143 would issue excessive "The Service Initiator service has reported an invalid current state 0." (Event ID: 7016) messages in the Windows Event Viewer system logs. (Case N10229)

Version 5.3.0 N1

This is the initial release of this product. The following features are included:

- Added License Verification Software facility.
- Added genMAC.exe to the EFT143 product distribution file set.
- Added support for the NetEx/IP network protocol.
- Enhanced product to run on both Windows NT and Windows 2000.

Appendix A. Distribution Contents

Windows NetEx/eFT is distributed on one 3 ½" diskette. During installation, the following files are installed:

```
C:\SICOMNT\USER
Server.exe        = executable  NETEX-eFT Server for TCP/IP.
Client.exe        = executable  NETEX-eFT Client for TCP/IP.
Alias.ua          = alias help file.
Example.ua        = sample NetEx/eFT aliases.
NTHELP.ua         = NT/Win2K specific help text.
Prodconf.ini      = NetEx/eFT product configuration file.
Sclient.ua        = sample site startup for  NETEX-eFT Client.
Sserver.ua        = sample site startup for  NETEX-eFT Server.
Userhelp.ua       = general help text .
Verify.ua         = NetEx/eFT verify script.

C:\SICOMNT\SI
SvcInit<NET>.exe  = executable  NETEX-eFT Service Initiator.
SIConfig          = Service Initiator config file.
Svciserv<NET>.exe = Service Initiator Service executable.
Svcmsg.dll        = Service Initiator Service messages file
Setup.exe         = Service Initiator Service install application.
SILog.exe         = Service Initiator log file viewer.
```

The following utility is also on the distribution media:

```
genMAC.EXE        = utility used to obtain platform fingerprint.
```

Appendix B. Internal Functions

Service Initiator

Most NetEx/eFT products install an application called the Service Initiator, or NETEX-eFT Service Initiator. The Service Initiator is a simple process that posts a listen on a specific TCP/IP socket, waiting for a connection request from a remote host. When the request is received, the Service Initiator:

- Verifies the UserID and password is valid by logging the user into the local system.
- Starts a NETEX-eFT Responder (Server) on the local machine with a unique socket address. The Responder then posts a listen on the unique socket address and waits for the remote login.
- Informs the calling process (remote client) of the unique socket address, and verification code that the Responder is waiting on. The remote client then connects to the Responder and the session is established.

The Service initiator should always be running waiting for connection requests. Without a Service Initiator running, a remote NetEx/eFT client cannot connect to the local machine.

The standard method for starting a process at system startup on Windows NT and Windows 2000 is via an NT/Win2K Service. Once an NT/Win2K Service is installed, it may be started automatically each time the Windows NT or Windows 2000 OS initializes. Furthermore, NT/Win2K Services do not terminate when a user logs off. Under Windows NT/Win2K, an application that is not an NT/Win2K Service does not start until a user physically logs onto the local NT/Win2K system, and terminates when the user logs off. Therefore, a Service Initiator not running as an NT/Win2K Service could not allow access to an NT/Win2K machine that did not have a user physically logged on.

Service Initiator Service

NetEx/eFT for Windows NT and Windows 2000 includes a Service Initiator (NETEX-eFT <NET> Service Initiator) and also a Service that starts the Service Initiator at system boot (NETEX-eFT <NET> Service Initiator Service or eFTSvcInit<NET>). The install program automatically installs the Service Initiator Service as an NT/Win2K Service with startup properties of Automatically, which means that the eFTSvcInit<NET> application will start when the NT/Win2K system is initialized. The Service Initiator Service then starts the standard NETEX-eFT <NET> Service Initiator.

By default, any process running under an NT/Win2K Service does not have access to a desktop or console. Therefore, the output from the Service Initiator will be kept in a log file called SvcInit.log. To view the Service Initiator log file, run the "NETEX-eFT <NET> SI Log" utility. The Service Initiator log files are kept in the same directory as the Service Initiator executable (by default this is *C:\SICOMNT*\SI where *C:\SICOMNT* is the NetEx/eFT install directory).

The Service Initiator can be controlled via the Services application in the Windows NT/Win2K Control Panel. By default, the Service Initiator will start automatically each time Windows NT/Win2K is initialized. The Service application startup panel allows you to change the startup parameter to manual or disabled. As installed, the Service Initiator runs under a default SYSTEM ID. The UserID and password for each NETEX-eFT Responder is passed on the connection request. Therefore, do not change the default UserID for the Service Initiator Service. You may stop, pause, and restart the Service Initiator from the

Services application. Each time the Service Initiator is started or stopped, a message is posted to the Windows NT/Win2K Application Event Log with a source of eFTSvcInit<NET>.

Service Initiator Service Event Log Messages

The following NT/Win2K Application Event Log messages may be generated by eFTSvcInit<NET>.

Source	ID	Type	Message	Explanation
eFTSvcInit<NET>	4200	Info	The Service Initiator has started	Normal start message.
eFTSvcInit<NET>	4201	Err	Failed to start Service Initiator with error code N	A call to the NT/Win2K Service Manager failed.
eFTSvcInit<NET>	4206	Info	Service Initiator restarting	The service is restarting after a pause.
eFTSvcInit<NET>	4292	Err	CreateProcess failed with error Code N	The call to create the NETEX-eFT Service Initiator process failed.
eFTSvcInit<NET>	4298	Info	Service Initiator Paused	The service has been paused.
eFTSvcInit<NET>	4299	Info	Service Initiator terminates with status 0	Normal termination message.

Install and Delete of the Service Initiator Service

The file Setup.exe, installed in the NetEx/eFT SI directory (C:\SICOMNT\SI\Setup.exe) is an install utility to install or uninstall the NETEX-eFT <NET> Service Initiator service. The syntax to remove the service is:

```
SETUP delete
```

The syntax to install is:

```
SETUP create C:\SICOMNT\si\Svciserv<NET>.exe
```

Where C:\SICOMNT is the NetEx/eFT install directory. You must first delete a currently installed NETEX-eFT <NET> Service Initiator Service prior to installing a new version. The setup utility installs the module Svciserv<NET>.exe as an NT Service. It will also add an entry to the Registry under:

```
HKEY_LOCAL_MACHINE\
      system\
            CurrentControlSet\
                  Services\
                        EventLog/
                              Application
```

called eFTSvcInit<NET> that denotes the location of the NETEX-eFT <NET> Service Initiator Service Event Log Message file.

If for any reason the NETEX-eFT <NET> Service Initiator does not stop when the eFTSvcInit<NET> Service stops, the Service Initiator may be stopped by connecting to it using a NETEX-eFT client and the following connect command:

```
NTXeFT> CONNECT  hostname -!control stop
```

Service Initiator Startup Parameters

When the Service Initiator starts up it opens a file SIConfig to determine what TCP/IP services to offer and how to start services when a connect request is received. The default SIConfig file shipped with NetEx/eFT contains the following information.

```
*
* Svc       Keyword           Value
*-----      -----------       ---------------------------------------------
NTXeFT      SERVER            %r\..\user\server.exe -ser %s -si
            VERBOSE           YES
            MINIMIZE          YES
            DETACH            YES
*           TRACE             0123456789ABCDEF
*
```

An asterisk character, '*', denotes a comment. In this example, the Service Initiator offers one service:

- NTXeFT or 6900 starts the NETEX-eFT Responder (SERVER).

The following options may be selected:

- VERBOSE - Generate verbose output of startup.
- MINIMIZE - Start the application minimized. This is not applicable unless the service is not detached.
- DETACH - Start the application as a hidden process. When detach is set to NO (or not defined) the process has access to the application desktop. For example, starting a process with MINIMIZE YES and DETACH NO causes an icon to appear on the desktop when the process is started.

Service Initiator Security

When a remote host attempts to connect to the NETEX-eFT <NET> Service Initiator, a UserID and password are required. The Service Initiator then verifies the user against the NT/Win2K security system and passes a logon token with the security profile to the NETEX-eFT Responder process. The NETEX-eFT Responder then operates in the context of the UserID passed on the connect command. To validate the user, the account must have the "Log on locally" privilege.

Starting the Service Initiator on the Desktop

In order for the Service Initiator to access the NT/Win2K security system, it must be started by a UserID that has the required privileges to authenticate UserIDs. When the Service Initiator is started as a service running in the Local System account (the default NetEx/eFT Installation), it will already have these privileges.

You may run a stand alone Service Initiator by passing the -SECURITY OFF option on the Service Initiator command line. However, all processes connecting to the Service Initiator will run in the context of the currently logged on UserID.

To run the Service Initiator on the desktop with security, the process starting the Service Initiator must have the following privileges:

Privilege	Display Name
SeTcbPrivilege	Act as part of the operating system
SeAssignPrimary	Replace a process level token
SeIncreaseQuota	Increase quotas

The required privileges can be added to an account by using the "User Rights Policy" dialog box. Run the User Manager and choose User Rights from the Policies menu to see the dialog box.

Note: You must select the "Show Advanced User Rights" check in box to see these privileges.

NT/Win2K Security

Windows NT/Win2K File System (NTFS) is a secure file system. All files and directories on an NTFS volume contain information regarding access permissions, ownership, and auditing. This security information can prevent users from being able to access the files.

NetEx/eFT requires a UserID and password that is validated against the local Windows NT/Win2K Security System. Windows NT/Win2K will validate all attempts by NetEx/eFT to access the files and resources against the logged-in UserID and password.

Appendix C. Network Security and NetEx/eFT

If your network solution includes firewall support or other IP-based filters (bastion host, screening router, etc.), the NetEx/eFT product architecture allows you to securely establish and run NetEx/eFT connections with high performance and ease. NetEx/eFT allows administrators to hide this network issue from the end user by altering the NetEx/eFT configuration file, ("SIConfig"), which was installed with your NetEx/eFT client software.

You, as a NetEx/eFT administrator, have to provide an available port to the NetEx/eFT client by specifying a startup parameter (%s) for a NETEX-eFT server in the configuration file on a NetEx/eFT client computer. However, if you are going to run more that one task on a client simultaneously, you have to specify a port range in a configuration file on a NetEx/eFT client computer by inserting a new parameter called **PORTRANGE**

The following examples show these modifications.

Specifying One Port Number

After the change, the NetEx/eFT client will access the NETEX-eFT server using port 3000.

Important: You must stop the service initiator before making this change; restart the service initiator after the configuration modification is complete

Original line in configuration file:

```
      NTXeFT      SERVER      %r/../user/server.exe -ser %s –si
```

Customized line in configuration file:

```
      NTXeFT      SERVER      %r/../user/server.exe -ser 3000 -si
```

The following example is an expanded view of a Windows NT/Win2K configuration change.

File SIConfig *before* changes:

```
* SVINIT configuration:
*
* Svc       Keyword           Value
*-----      --------------    ------------------------------------------------
 NTXeFT     SERVER            %r\..\user\server.exe -ser %s -si
            VERBOSE           YES
            MINIMIZE          YES
            DETACH            NO
*           TRACE             0123456789ABCDEF
*
```

File SIConfig *after* changes:

```
* SVCINIT configuration:
*
* Svc       Keyword           Value
*------     --------------    ----------------------------------------------
 NTXeFT     SERVER            %R\..\USER\SERVER.EXE -SER 3000 -SI
            VERBOSE           Yes
            MINIMIZE          YES
            DETACH            YES
*           TRACE             0123456789ABCDEF
*
```

Specifying a Port Number Range

After the change, the NetEx/eFT client will access the NETEX-eFT server using any port from 3000 to 3010.

Important: You must stop the service initiator before making this change; restart the service initiator after the configuration modification is complete.

Note: Be sure that the line for specifying a NETEX-eFT server does NOT have a specified port number. The line in the configuration file should be:

```
      NTXeFT      SERVER      %r\..\user\server.exe -ser %s -si
```

New customized line in configuration file:

```
      PORTRANGE   3000:3010
```

The following example is an expanded view of a Windows NT/Win2K configuration change.

File SIConfig *before* changes:

```
*     SVCINIT configuration:
*
* SVC       Keyword           Value
*------     ------------      ------------------------------------------
 NTXeFT     SERVER            %r\..\user\server.exe -ser %s -si
            VERBOSE           YES
            MINIMIZE          YES
            DETACH            NO
*           TRACE       0123456789ABCDEF
*
```

File SIConfig *after* changes:

```
*     SVCINIT configuration:
*
* Svc       Keyword           Value
*------     -------------     ----------------------------------------------
 NTXeFT     SERVER            %r\..\user\server.exe -ser %s -si
            VERBOSE           YES
            MINIMIZE          YES
            DETACH            NO
            PORTRANGE         3000:3010
*           TRACE             0123456789ABCDEF
*
```

Appendix D. Product Configuration File

Each NESi software product that has integrated the License Verification Software facility now contains a product configuration file. The NetEx/eFT product includes this file in its installation distribution file set. During installation, this file (Prodconf.ini) is installed in the USER subdirectory of the installation directory, which defaults to C:\SICOMNT.

The default Prodconf.ini file shipped with NETEX/eFT contains the following information:

```
# Network Executive Software, Inc.
# EFT Product Configuration file
LICPATH      C:\Winnt\NESikeys.ini  # NESi License Key file
```

A '#' character denotes a comment. Non-comment records must contain a keyword/value string. The initial version of this file contains only a single keyword/value record:

- LICPATH – this keyword defines the full path to the NESi License Key File (see Appendix E).

Appendix E. License Key File

A single NESi License Key file must reside on each NT/Win2K system on which one or more NESi products containing license support will be installed. The following guidelines apply:

- The default file name is **NESikeys.ini**.
- The **LICPATH** keyword/value pair in the product configuration file (see "Appendix D. Product Configuration File") specifies the full path name to this file. The default is: **C:\Winnt\NESikeys.ini** .
- The NT/Win2K System Administrator must initially create this file prior to invocation of NetEx/eFT components such as Service Initiator and Client.
- A leading '#' character in a file record denotes a comment line.
- The NT/Win2K System Administrator must edit this file to add a new encrypted Software Key each time such a key is obtained from NESi for the EFT143 product (and other license-enabled NESi products). This should be done prior to installing the product, and must be done prior to being able to run the product successfully.
- The file may contain multiple keys per product due to new product releases or a change to the platform's fingerprint (on NT/Win2K, the MAC address of a configured network card). To make the file easier to maintain over time, it is recommended that you precede each Key entry with a comment line that documents the product and release level of the product that the key is associated with. It will then be easier to delete older Keys that are no longer valid for the product.
- The following shows an example of what a NESikeys.ini file might look like after adding several Keys to the file:

```
# Network Executive Software, Inc. Software License Key file
# Key for EFT143 N1 (1-15-03):
86481096ff6c3ebb9b34099b7e639fef
# Key for EFT143 pre-release (3-30-01):
e0fef4aaae2aa01e3d7f35d53039612da5e4abcd05a829a4
```

Appendix F. Obtaining Platform Fingerprint via genMAC

The utility genMAC.exe is packaged in the EFT143 product distribution media in order to enable the NT/Win2K system administrator to obtain a "fingerprint" of the platform on which EFT143 is to be installed. This fingerprint must be submitted to Network Executive Software in order to obtain a valid encrypted Software Key for the EFT143 product. The encrypted Software Key obtained from NESi will provide a valid license of the current release of the EFT143 product on the NT/Win2K platform on which it is to be installed.

On Windows NT and Windows 2000, a platform fingerprint consists of the MAC address of an installed network interface card. To obtain a list of one or more platform fingerprints, do the following:

1. Insert the NetEx/eFT installation disk into your Windows NT/Win2K machine (e.g. A: drive).
2. From a MS-DOS Command Prompt window, invoke:

   ```
   A:\genMAC
   ```

   The genMAC utility will display output similar to the following:

   ```
   **  genMAC displays one or more platform 'fingerprints'.
   **  A network adapter MAC address is a fingerprint.
   **  The fingerprint(s) detected on this platform follow:

         'Ethernet' adapter MAC address: 0000e898eca9

   **  end of genMAC report. **
   ```

3. Choose one of the fingerprints that were displayed (e.g. "0000e898eca9") and submit it to NESi in order to receive a valid encrypted Software Key for the current release of the EFT143 product.