eFT213 NetEx/eFT™

for IBM z/OS™ Systems

Release 5.5

Memo To Users

May 2021

6450 Wedgwood Road North #103
Maple Grove, MN 55311

Document Revision Record

Revision	Description
01 (01/2001)	Manual modified for NESi ownership.
02 (01/2001)	Reformat using nesi_man.dot (12/15/00) template.
03 (04/2005)	• Updated for conversion to eFT product. • All documentation changes noted in Memo To Users from prior releases added. • Addition of FTP alias commands. Other minor grammatical and formatting changes.
04 (06/2006)	• Updated copyright year. • Changed references to "//SYSIN DD" in JCL examples to "//STDIN DD". General format changes for better readability.
05 (11/2009)	• Corrections for release 5.4 • Updates copyright year. • ISPF Panels supported. • 0Cx on very long passwords corrected • 0Cx on very long variables corrected • Command length issues documented CLIST allocations of STDIN should be changed to include a blocksize equal to or greater than the screen size of the 3270 model that you are using. i.e., `ALLOC F(STDIN)  DS(*) REUSE BLKSIZE(4096) RECFM(U)` • DEBUGON & DEBUGOFF aliases added • DBGON & DBGOFF scripts added
06 (08/2011)	Added missing eFT213 message "EFT213-2536" to message table.
07 (11/2011)	Corrections to show command output; support for new licensing beginning in Release 5.4.4
5.4.5 (05/2012)	Miscellaneous updates in preparation for eFT213 5.4.5 release.
5.4.7 (6/2018)	eFT213 5.4.7 release.
5.5 (5/2021)	eFT213 5.5 release; Separately licensed Secure connections feature added.

Table of Contents

Introduction

This product implements the Network Executive Software eFT213 product. This version contains a separately licensed feature that enables TCP/IP encrypted data transfers between the client and the server. If secure transfers are not required, your current license keys will continue to function.

This document contains:

- Software and installation related service notes
- Installation instructions
- Installation verification procedures
- Post installation considerations
- A description of the distribution contents
- A summary of updates to this version
- Listings of the installation jobs and configuration parameters

For more information on using NetEx/eFT please refer to the publication:

eFT213 NetEx/eFT™ for IBM z/OS™ Software Reference Manual.

New Features

A list of new features included with this release.

- Optional secure transfers are supported for IP installations.
- Refer to the Update Summary at the end of this document for a list of updates contained in this release.

Service Notes

Known problems and issues with this release:

- eFT has changed the default service name (TCP/IP service name or NetEx OFFER name). The new names are “EFT” or “eft” defaulting to port number 6900, and “EFTS” and efts” defaulting to port number 6910 for securely encrypted connections. Users of the USER-Access product will recall that the service name was “USER” or “user”. Any site wishing to run eFT in a mixed environment with existing USER-Access hosts must take steps to modify the installation job and software configuration as necessary.
- Data sets or files containing binary (non-character) data should not be transferred using “MODe CHAracter”. This was not recommended with previous versions of eFT either. Truncated records may occur during character mode file transfers due to the internal file transfer protocol, which improves performance when transferring to or from an ASCII host.

  Use “MODe RECord” transfer for z/OS to z/OS binary data file transfers, or “MODe STReam” for hosts not supporting record mode. If record or stream mode does not meet your processing requirements, try “MODe V1Char” which tends to be more compatible with binary data transfers.
- z/OS data sets used for eFT parameter or command input must not contain sequence numbers, including JES SYSIN data. Data sets used in file transfers may contain sequence numbers.
- The LOCAL command qualifier “-PREFix” is not used in eFT213.
- When executing eFT in a z/OS native batch environment setting the local or remote “DIRectory” or “TSOPREFix” has no effect and will always show a null value. “DIRectory” and “TSOPREFix” are only valid in a TSO/E batch or TSO/E online environment.
- The eFT QUIT command sets the following z/OS condition codes:

Quit	Issuing QUIT with no operands sets the condition code based upon the completion status of the prior eFT command.
Quit Success	Sets condition code zero (0).
Quit Warning	Sets condition code four (4).
Quit Error	Sets condition code eight (8).
Quit Fatal	Sets condition code twelve (12).

  No other condition code values are supported at this time.

- C and PL/I Language run time environment ABENDs

  S806 Issued if an eFT program or support routine cannot successfully load a run time module. Determine the module name associated with the S806 ABEND and check to ensure that module is available at your site in via the link pack area (LPA), system link list concatenation, a JOBLIB DD statement, or STEPLIB DD statement. Use the following list to help determine which library the module normally resides in:

PLIxxxxxx	PL/I Library run time module: CEE.SCEERUN
IKJxxxxx	TSO/E run time module: SYS1.LINKLIB or SYS1.LPALIB
ISPxxxxx	IPSF run time module: ISP.SISPLOAD
NUAxxxxx	eFT module: EFT.N24.LOAD
EFTxxxxx	eFT module: EFT.N24.LOAD

- The –CREATE qualifier value “NEW” is invalid when used in conjunction with the -VOLUME qualifier when sending or receiving files to a tape data set.
- zOS account command hangs terminal (client in loop) Ticket 8685
- Allow use of non-secure Netex sessions Ticket 9033

Installation

Prerequisite Products

eFT213 release 5.5 requires:

- IBM OS/390 version V2 R10 (or higher) or IBM z/OS version 1.1 (or higher) be fully installed, tested and running on your system.
- ISPF version 3.3.0 (or higher).
- One of the following network products is fully installed, tested and running on your system.
  - For NetEx Installations: Network Executive Software NetEx H210IPZ version 7.0 (or higher).
  - For IP Installations: IBM Communications Server TCP/IP. OS/390 OpenEdition TCP/IP sockets are not supported by this version of eFT213. Refer to the IBM Communications Server publications for more information.
- In addition to the above product prerequisites, the eFT213 installation procedure uses the following IBM z/OS products and utilities:
  - The background TSO/E Terminal Monitor Program (TMP) IKJEFT01.
  - The Assembler program IEV90 for Assembler H, or ASMA90 for the High Level Assembler.
  - The Linkage Editor program IEWL.
  - The Utility programs IEBGENER, IEBCOPY and IEFBR14.
  - The Access Method Services command REPRO.

Installation Notes

NetEx Software eFT213

- This version of eFT213 allows for optional secure data transfers in TCP/IP installations.
- Please review the "Update Summary" on page 47.
- DASD Space Requirements

  eFT213 requires about 40 megabytes (80 3390 cylinders) of DASD space for installation and configuration.

- z/OS Region Size Requirements

  Running an eFT Client or Standalone Server program as a native batch job requires approximately 2048K (kilobytes). Running an eFT Client, Helper or Standalone Server program under control of TSO/E, either online or batch, requires approximately 4096K. Larger region sizes may be needed to execute local and remote TSO/E commands or z/OS programs.

  The Multiplex Server requires approximately 4096K, but may require a larger region to support a greater number of concurrent sessions.

- Root Directory Data Set

  The eFT Root Directory data set name is provided via the ROOT(...) or TEXT(...) parameter in the installation job.

  The eFT site start up files SCLIENT and SSERVER, the help files MVSHELP and EFTHELP, and the NetEx message file NETEXMSG must reside in the Root Directory data set.

  All eFT jobs, started tasks, and both local and remote users will require a minimum of "read" level security access to the Root Directory data set.

  The Root Directory data set name is imbedded as a constant in the eFT213 load modules by the installation job. Because of this, the Root Directory data set cannot be renamed without also updating the eFT213 load module. To update the Root Directory data set name in the load modules any time after initial installation, you must tailor and run the LINK phase of the installation job **or** include a TEXTLIB DD statement in batch jobs, or dynamically allocate TEXTLIB under TSO. A TEXTLIB DD statement is contained in all clists and batch JCL jobs included in the distribution.

- The "Client" Program

  Most z/OS users of eFT will run the Client program NUACLIEN from the data set defined via the LOAD(...) parameter in the installation job. z/OS Client jobs and users will require a minimum of "execute" level security access to that data set.

  Executing the Client in batch does not interface with VTAM or TSO/E allowing z/OS users to execute eFT without VTAM or TSO/E being active. Local TSO/E commands are not supported in this environment. z/OS programs can be run via the LOCAL command provided there are no DD name conflicts with eFT. A local z/OS program is passed the standard z/OS parameter area consisting of two bytes of length followed by the actual parameter text. Example JCL to execute the Client program in batch is provided in the EFT.N24.TEXT dataset installed as part of the distribution.

  Executing the Client in batch under control of TSO/E does not interface with VTAM allowing z/OS users to execute eFT without VTAM being active or using VTAM resources. Local TSO/E command execution is supported, with the normal TSO/E batch restrictions (i.e. the TSO/E TERMINAL command is not supported, etc.). Example JCL to execute the Client program in batch under control of TSO/E is provided in the EFT.N24.TEXT dataset installed as part of the distribution.

- The “Multiplex Server” Programs

  The Multiplex Server is the eFT facility a remote host Client program will normally CONNECT to. The primary functions of the Multiplex Server are to:

  - Continuously OFFER a network service or LISTEN on a port
  - Accept a network CONNECT request from a remote host
  - Logon the remote user to TSO/E and start the Helper program
  - Pass remote user requests to the Helper program
  - Return TSO/E command output to the remote user
  - Logoff a remote user from TSO/E and DISCONNECT the network session
  - Manage multiple concurrent remote user sessions
  - Produce a log of events.

  The Multiplex Server loads and executes multiple program modules from the data set defined via the LOAD(...) parameter in the installation job. The Multiplex Server job or started task will require a minimum of “execute” level security access to that data set.

  It is recommended that the “TIME=1440” keyword be left on the JOB and EXEC cards in the Multiplex Server JCL, since it is usually left active for the duration of a z/OS IPL. You may also need to add accounting information to the EXEC card in the Multiplex Server started task JCL, if your security system or z/OS exits require it.

  It is recommended that you set the Multiplex Server to a relatively high dispatching priority on your z/OS system, usually just below VTAM, NetEx, and/or TCP/IP. The Multiplex Server resource utilization is minimal since most eFT activity (including file transfer) occurs under and is reported against the remote user’s TSO/E session.

  eFT CONNECT command processing has an internal timeout value of 60 seconds. The network CONNECT sequence between the remote host Client program and the Multiplex Server must be completed in that interval. If the Multiplex Server is swapped by z/OS for a long period or is not given sufficient z/OS resources to complete the CONNECT sequence, a network or eFT error message is issued and the connection is failed. Note that only the initial network CONNECT sequence is affected and that the rest of the eFT CONNECT command processing, including TSO/E logon time, is controlled via the MUXLOGTO(...) parameter in the installation job.

  The following differences between the eFT Multiplex Server JCL and the USER-Access Multiplex Server JCL should be noted:

  - The PRODCONF DD statement, identifying the location of the software key, must be included in the eFT Multiplex Server JCL. Please refer to “The PRODCONF DD/file”. for a description of the format and contents of the PRODCONF file.
  - STDERR and STDOUT DD statements must be included in the eFT Multiplex Server JCL. These DD statements are in addition to the existing SYSERR and SYSOUT DD statements. The format of these statements is as follows:

    ```
    //STDOUT    DD SYSOUT=*
    //SYSOUT    DD SYSOUT=*
    //STDERR    DD SYSOUT=*
    //SYSERR    DD SYSOUT=*
    ```

    Caution: DCB information should not be specified on the //STDOUT, //SYSOUT, //STDERR, and //SYSERR DD statements.

- The EFTMCONF DD statement, identifying the location of the EFTMCONF control file, and must be included in the eFT Multiplex Server JCL. Please refer to "Step 12. Customize TSO Remote Logon Files " for a description of the format and contents of the EFTMCONF file.
- The EFTVCONF DD statement, identifying the location of the EFTVCONF control file, and must be included in the eFT Multiplex Server JCL. This file is tailored by the install process and normally does not require further configuration.
- The EFTMLOG DD statement, identifying the destination for the servers log output, and must be included in the eFT Multiplex Server JCL.
- EFTMCONF, EFTVCONF, and EFTMLOG DD statements replace the NUAMCONF, NUAVCONF, and NUAMLOG DD statements from older products.
  - EFTMCONF is the multiplex server configuration file.
  - EFTVCONF is the vtam interface configuration file.
  - EFTMLOG is the output file from the multiplex server.

- The "Helper" Program

  All remote users of eFT will run the Helper program NUAHELPR from the data set defined via the LOAD(...) parameter in the installation job. All remote user TSO/E sessions will require a minimum of "execute" level security access to that data set (HLQ.load).

  The Helper program is automatically started by the Multiplex Server after TSO/E logon is complete. The Helper program executes remote Client program requests, including file transfers and remote command execution.

- The "Standalone Server" Program

  z/OS jobs or users may run the Standalone Server program NUASSERV from the data set defined via the LOAD(...) parameter in the installation job. Any z/OS job or user executing the Standalone Server will require a minimum of "execute" level security access to that data set.

  The Standalone Server can be used in place of the Multiplex Server or can execute concurrently with the Multiplex Server. The Standalone Server is not a direct replacement for the Multiplex Server, since it only remains active for one remote user session (i.e., when the remote user disconnects, the Standalone Server job step will terminate). Also, the Standalone Server is not designed to return TSO/E command output to the remote Client program. The Multiplex Server is required to provide full support for returning TSO/E command output.

  It is recommended that each Standalone Server job use a unique network service name or port number and that no Standalone Server service name or port number match a service name or port number used by a Multiplex Server. Coding the same service name or port number for many servers will result in an error or in remote users randomly connecting to any available matching service name or port number. This usually causes confusing or undesirable results for remote users.

  Executing the Standalone Server in batch does not interface with VTAM or TSO/E allowing remote users to connect to eFT without VTAM or TSO/E being active, but without remote TSO/E command support. Remote z/OS programs can be run as REMOTE commands provided there are no DD name conflicts with eFT. A remote z/OS program is passed the standard z/OS parameter area consisting of two bytes of length followed by the actual parameter text. The z/OS program completion code is returned to the remote user but no z/OS program output is returned. Example JCL to execute the Standalone Server program in batch is provided in the EFT.N24.TEXT dataset installed as part of the distribution.

  Executing the Standalone Server in batch under control of TSO/E does not interface with VTAM allowing remote users to connect to eFT without VTAM being active or using VTAM resources. Remote TSO/E command execution is supported and remote command status is returned to the remote user, but

TSO/E command output is not. Example JCL to execute the Standalone Server program in batch under control of TSO/E is provided in the EFT.N24.TEXT dataset installed as part of the distribution.

- The ISPF Interface

  The eFT ISPF interface requires three temporary work data sets for each user during execution. The amount of DASD space required for each work data set will be about 40 kilobytes. The DASD unit name assigned to these work data sets is defined via the ISPFUNIT(...) parameter in the installation job. Specifying "ISPFUNIT(' ')" is valid and will cause the work data sets to be allocated using the default unit name from each user's TSO/E profile. It is recommended that these data sets be allocated to a Virtual I/O (VIO) unit at your site.

IBM VTAM

- eFT213 requires a set of VTAM application nodes be defined and active. The nodes are used by the Multiplex Server for remote user logon to TSO/E. One node is required for each concurrent remote user session. The nodes are used on the local VTAM host only and do not require any VTAM cross-domain definitions.

  The EDIT phase of the installation job creates a sample set of VTAM application node definitions and the COPY phase copies them into your VTAM configuration library for later activation.

- Shutting down VTAM with the "Z NET,QUICK" z/OS console command will cause the eFT Multiplex Server to attempt to open each of the VTAM application nodes at regular intervals, which can result in a lot of z/OS console traffic. It is recommended that the Multiplex Server be shut down before VTAM is halted or that the "MUXWTO(NO)" parameter be specified in the installation job.

- If the Multiplex Server VTAM application nodes are varied inactive after Multiplex Server initialization, the Multiplex Server will try to reopen the inactive node at regular intervals. A problem has been reported that some versions of VTAM leave a 48 byte area of z/OS Common Storage Area (CSA) allocated for each unsuccessful open. There are numerous VTAM fixes available from IBM which correct CSA related problems, but none have been specifically identified to fix this particular problem. If the Multiplex Server nodes are always left active you should not experience this problem.

- Installing a new version of VTAM does not usually require any changes to eFT. Ensure that data set SYS1.VTAMLST(EFTVAPPL) is installed correctly for the new VTAM version. If the eFT node names changed in data set SYS1.VTAMLST(EFTVAPPL), you may need to tailor and run the EDIT and COPY phases of the installation job.

IBM TSO/E

- The local client supports long passwords (passphrase). The remote connection to another z/OS does not support long passwords. This is an IBM restriction. eFT uses a linemode connection on the remote z/OS system. IBM does not support passphrases in linemode. This will result in repeated INVALID PASSWORD messages.

- Line mode TSO/E is the z/OS interface that will be presented to the remote user and is required for local and remote command execution. The TSO/E environment was selected for eFT instead of CICS, IMS, etc., because it provides a consistent z/OS "command language" and provides a flexible and secure environment for remote user activity.

- eFT does not support a fully "interactive" TSO/E logon process for remote users. The Multiplex Server execution parameters in the Multiplex Server configuration file found in the EFT.N24.TEXT dataset installed as part of the distribution should be reviewed to ensure the correct action is taken for any messages generated by your TSO/E logon process. For more information read section "The Multiplex Server and TSO/E Logon Processing" on page 43.

- Remote eFT users are logged onto TSO/E as a line mode terminal (3767, TTY, NTO, etc.) and not as a 3270 device. Logon keyword values normally supplied on the TSO/E 3270 full screen logon panel are not available during line mode logon. Any logon information that is "remembered" by the full screen logon panel, such as account information, must be provided by the remote user on the eFT CONNECT command. This is especially true in a RACF environment, where the remote user must supply an account number and TSO/E logon procedure name during eFT CONNECT processing. Specific values for account and procedure name can be provided on the CONNECT command using the "ACCount" and "PROFile" qualifiers. Site defaults for account and procedure name can also be provided in the Multiplex Server execution parameters. See the EFTMCONF configuration file found in the EFT.N24.TEXT dataset installed as part of the distribution.

- TSO/E logon "pre-prompt" exits or initial TSO/E commands which do not properly check for terminal type before outputting a 3270 data stream may cause remote user logon problems. This type of logon problem can usually be handled by defining additional eFT logon keywords.

- Prompting, character translation, screen size, the line delete character, and the character delete character are turned off in the user profile for any TSO/E user ID accessed from a remote host. These changes are necessary to ensure eFT protocol exchanges between the Multiplex Server and the Helper programs are not inadvertently corrupted or translated by TSO/E. If the same user ID is used for 3270 terminal access (ISPF, etc.), these profile changes usually do not affect 3270 operations. If the changes do present a problem, is it suggested that an initial TSO/E logon CLIST be provided for the affected user ID(s) which sets the profile to the desired 3270 values. The eFT profile changes are made after the initial TSO/E logon command or CLIST has completed, and will only be performed when the user ID is used from a remote eFT host.

- eFT only supports line mode TSO/E applications for remote command execution. Full screen 3270 applications (ISPF, ISPF/PDF, etc.) will either not initialize correctly or produce unpredictable results on the remote user's terminal. Also, TSO/E commands or CLISTs which prompt the user for input are not currently supported as remote commands by eFT.

  eFT does not require any data sets to be pre-allocated in TSO/E logon procedures used by remote users. eFT remote users can be logged onto TSO/E using a minimal logon JCL procedure similar to:

```
//EFTPROC  PROC
//EFTUSER  EXEC PGM=IKJEFT01,DYNANMBR=20
//SYSPROC  DD DSN=SYS1.CMDPROC,DISP=SHR
```

  The SYSPROC allocation should include all the TSO/E CLIST and REXX libraries the remote user might need for eFT remote command execution.

  Using the above logon procedure can save considerable time and resources over "standard" logon procedures which perform data set allocations for ISPF, ISPF/PDF or other full-screen applications.

- TSO/E accounts used for eFT will require TSO/E mount authority if the account will be accessing data stored on tape. Mount authority is the recommended approach to allow access to z/OS tape based data for remote users.

  Most z/OS sites are not familiar with allowing TSO/E online tape mounts, and in the simplest case allowing mounts requires changing the user's TSO/E attributes in the SYS1.UADS data set or security system user profile. Your security system may also need other updating to allow the affected user ID(s) access to tape related resources.

  Allowing mounts does not change or circumvent a TSO/E user's security access authority. Allowing mounts only provides direct allocation of tape devices to the TSO/E session. The z/OS console operator has the ability to cancel the TSO/E user's mount request without canceling the entire TSO/E Session. eFT recognizes the canceled mount request and returns a descriptive error message to the remote user.

  If TSO/E mount authority cannot be granted, the eFT Standalone Server can be submitted as a batch job to allow access to tape data. This provides full functionality for the remote user, but causes a remote

interactive request to wait for JES to schedule the Standalone Server job to an initiator. If the submitted Standalone Server job fails or is canceled, eFT has no way of notifying the remote user, who may be waiting for the network connection to complete. This typically leads to frustration for the remote user and is not the recommended solution.

- Installing a new version of TSO/E does not usually require any changes to eFT.

  If your VTAM node name for the new version of TSO/E changed, you may need to tailor and run the EDIT and COPY phases of the installation job.

  The Multiplex Server execution parameters in the configuration file found in the EFT.N24.TEXT dataset should be reviewed to ensure the correct action is taken for any messages that may be generated by a new TSO/E logon process. For more information read section "The Multiplex Server and TSO/E Logon Processing" on page 43.

IBM ISPF and ISPF/PDF

- An ISPF interface to eFT is provided. This interface is designed to provide ISPF oriented users a familiar interface to the eFT Client program. It is not used by remote users when executing the Multiplex Server, Helper, or Standalone Server programs.
- When installing a new version of ISPF or ISPF/PDF, ensure that the ISPF interface CLISTs, panels, skeletons and messages are installed correctly for the new version of ISPF or ISPF/PDF. Pay particular attention to any ISPF or ISPF/PDF menus you changed during a prior eFT213 installation. To update your new ISPF or ISPF/PDF libraries, you may need to tailor and run the EDIT and COPY phases of the installation job.
- eFT dynamically invokes ISPF routines "ISPLINK", "ISPEXEC" and "ISPQRY". It is recommended that these modules be installed in your z/OS link list concatenation. eFT processing will continue successfully if any of these modules cannot be located, but z/OS error message CSV003I may be issued each time one of the modules is invoked.

IBM PL/I

eFT213 always requires the IBM run time environment for the PL/I Language to be available at your site.

- The PL/I Language run time environment is provided by the IBM Language Environment/370 (LE/370) product. It can be found in CEE.SCEERUN

Security Products

- eFT does not circumvent or bypass z/OS or TSO/E security. All of your current z/OS data set security and TSO/E logon security processes are fully honored by eFT. eFT213 is installed and fully functional at z/OS sites with basic z/OS security and at sites with security products of RACF and CA-ACF2.
- eFT213 client and server routines execute in z/OS problem program state (key 8) and do NOT require or enter z/OS supervisor state (key 0). eFT213 initialization does not use any z/OS authorized facilities and therefore does not require any z/OS authorization.

  The installation procedures suggest that the eFT programs may optionally be installed in the z/OS link list concatenation. This is suggested solely to remove the requirement of STEPLIB DD cards in user coded JCL, and not because eFT needs authorization.
- eFT does not have any special z/OS Common Storage Area (CSA) or Link Pack Area (LPA) requirements.
- Security access levels required for the eFT213 installation data sets are provided in section "NetEx Software eFT213" on page 9.

- eFT is designed to interface with TSO/E security products during remote user logon. Since eFT does not implement a fully "interactive" remote logon process, some security products may require that unique eFT logon keywords be provided during product installation.

  A separate set of logon keywords is provided for CA-ACF2 since that product has a unique TSO/E logon process, much different from TSO/E or TSO/E with RACF.

  For more information read section "The Multiplex Server and TSO/E Logon Processing" on page 43.

- eFT "LOGIN" aliases in remote site start up files may need to be changed to supply z/OS specific information such as procedure name, account number, etc.

- eFT batch jobs which connect to remote hosts may require a remote host user ID and password when connecting to the remote system. The user ID and password are usually supplied directly in the JCL via the SYSIN DD statement and the CONNECT command. If coding the user ID and password in the JCL present security problems, the CONNECT command, including the user ID and password can be placed in a z/OS sequential data set and then executed via the eFT INPUT command with the "ECHO off" qualifier. This sequential data set can be protected (via RACF, etc.), allowing read access to the appropriate batch job(s), and update access to only the "system administrator". All remote system passwords are then protected from computer operations, job scheduling, and other unauthorized personnel.

Storage Management Products

- During a file transfer, a z/OS data set that is a destination file will always be recalled from migrated or archived status. A z/OS data set that is a source file will only be recalled if the "RECALL" qualifier is set to "on" (the default). If "RECALL" is set to "off" or the recall of the migrated or archived data set is bypassed. If the recall is interrupted or canceled, the file transfer for that data set will fail with a descriptive eFT error message.

- eFT issues the DFHSM ARCHRCAL macro to recall migrated or archived data sets and the ARCHDEL to delete migrated or archived data sets. These two macros are issued regardless of the storage management product you have installed at your site.

For NetEx Installations: NetEx Software H210IP/H210IPZ NetEx/IP

- eFT213 is link-edited with your installed version of H210IP/H210IPZ in the LINK phase of the installation job. To link-edit with a new version of H210IP/H210IPZ anytime after initial installation, tailor and run the LINK phase of the installation job.

- The H210IP/H210IPZ subsystem name may optionally be changed by supplying a value for the "ADAPTer" qualifier on the eFT CONNECT command, or the "ADAPTER" keyword in the Multiplex Server execution parameters in the configuration file found in the EFT.N24.TEXT dataset. The "ADAPTer" qualifier can also be specified as an execution time parameter for the Standalone Server.

- The H210IP/H210IPZ initialization parameter "READTIME" usually requires changing for eFT.

  If you are planning to directly access tape data sets from eFT, you may need to increase the READTIME value in your z/OS NetEx initialization parameters. The default READTIME value of 60 seconds is usually exceeded during operator mounting of tape volumes. Set the READTIME value to the longest time needed for an operator to satisfy a tape mount request plus the time needed for any and all tape device positioning actions (rewind, forward space file, etc.).

  The NetEx READTIME value may also need adjusting if an eFT job or user can be swapped by the z/OS System Resource Manager (SRM) for long periods of time. Either assign the affected job or user a higher z/OS service level (via its performance group) or increase the z/OS NetEx READTIME value to the longest time a job or user could be swapped out.

  In summary, if a NetEx job or user remains in a z/OS related wait state (such as an extended I/O request or swap out) longer than the NetEx READTIME value, NetEx will disconnect the session. The NetEx

application, in this case eFT, will usually receive a NetEx NRBSTAT error code of 2306 or 3100 upon return from the mount, wait or swap.

For TCP/IP installations: IBM Communications Server (TCP/IP)

- eFT defaults to TCP/IP port number 6900 for its well-known port number for non-secure connections. Secure connections default to port 6910. Secure connections can only communicate with the port specified for secure connection. Non-secure connections can only communicate with the port specified for non-secure connections. The installation procedure will offer you the opportunity to specify the service names and port numbers to use. By default the service names “EFT”, and “eft”, are used in your TCP/IP configuration data set named similar to TCPIP.ETC.SERVICES. Refer to the IBM Communications Server publications for more information on service name coding.

  The port number will also need to be equated to service names “EFT”, and “eft” in your remote host TCP/IP definitions. It is important that all eFT TCP/IP hosts have the same well known port number defined.

Installation Checklist

Use the following checklist to provide your site specific names which will be used by the eFT213 installation job. The emphasized names are the names supplied in the distribution.

1. Select a set of high level qualifiers for the eFT213 product installation data sets.

   EFT.N24 _____

   Note: The following data sets will be deleted and recreated by the installation job if the default high level qualifiers of "EFT.N24" are chosen:

   EFT.N24.XMITLIB
   EFT.N24.TEXT
   EFT.N24.LOAD
   EFT.N24.LOADO
   EFT.N24.CLIST
   EFT.N24.ISPF
   EFT.N24.PANELS
   EFT.N24.SKELS
   EFT.N24.MSGS

2. Determine the z/OS unit name for an on-line DASD device to contain the eFT213 installation data sets. The unit or volume chosen should contain at least 40 megabytes (80 3390 cylinders) of available space.

   SYSALLDA _____

3. Determine the name of an IBM Assembler program (usually ASMA90 for the High Level Assembler or IEV90 for Assembler H) and the name of a Linkage Editor or Binder program (Usually IEWL, but may be HEWLKED for the DFSMS version of the Linkage Editor).

   ASMA90 _____

   IEWL _____

4. Determine the VTAM node name or ACB name for TSO/E (TCAS).

   TSO _____

5. Select the VTAM minor node names and the number of nodes to be assigned to the eFT Multiplex Server. The starting minor node name should end in three decimal digits and will be incremented by one for each additional node. The default values below will define nodes EFT001 through EFT010.

   EFT001 _____

   10 _____

6. Determine the NETWORK type (NETEX/TCP)

   NETWORK _____

7. Select the network service names and numbers to be offered by the eFT Multiplex Server and a different name or number for the Standalone Server sample jobs. Secure transfers are used only when the NETWORK type is TCP. Secure parameters can be ignored if the NETWORK is NETEX.

   EFT *(6900)* non-secure _____

   EFTSA Standalone non-secure _____

   Note: It is recommended that the default name of "EFT" be selected as the name offered by the Multiplex Server, because that is the name referenced in other eFT documentation.

8. Determine the name of the certificate data base. This is required for secure transfers. This may be either a GSKYMAN database defined on the system, or the USERID/KEYRING if using the RACF database. Contact your security administrator for the names.

   CERTDB _____

9. Determine the read password for GSKYMAN certificate data base. If you are using a RACF USERID/KEYRING this parameter MUST NOT be coded.

   CERTPW _____

10. Determine the host name to use when accessing the certificate data base. Required for secure transfers.

    CERTLB _____

11. Determine the data set name for the VTAM configuration data set. Coding ‘’ will prevent updating the library.

    SYS1.VTAMLST _____

12. Select the VTAM major node name that will contain the minor node name definitions.

    EFTVAPPL _____

13. Determine the data set name for the z/OS JCL procedure library used to start jobs from the z/OS operator console. Coding ‘’ will prevent updating the library.

    SYS1.PROCLIB _____

14. Select the started task procedure name that will be used to start the eFT Multiplex Server.

    EFTMSERV _____

15. Determine the data set name that all eFT users (both local and remote) will have access to for TSO/E CLIST execution. Coding ‘’ will prevent updating the library.

    SYS1.CMDPROC _____

16. Select the TSO/E command name that will be used to invoke the eFT Client program.

    EFT _____

    Note: It is recommended that the default name of “EFT” be selected as the TSO/E command name, because that is the name referenced in other eFT documentation.

Installation Procedure

The data set names supplied in the eFT213 sample JCL, CLIST and configuration parameters in the distribution are described below. You may modify the data set names to meet your site specific requirements provided you make the corresponding changes to the JCL, CLISTs and configuration parameters. The following installation instructions refer to the supplied data set names.

EFT.N24.XMITS This is the primary distribution file.

EFT.N24.XMITLIB This is a secondary distribution library.

EFT.N24.INSTALL This file contains the eFT213 installation job.

EFT.N24.LOAD This library contains the eFT213 program load modules.

EFT.N24.TEXT This library contains the sample JCL, CLISTs and configuration parameters needed for eFT execution.

EFT.N24.CLIST This library contains the TSO/E CLISTs for the eFT ISPF Menu System.

EFT.N24.PANELS This library contains the ISPF panels for the eFT ISPF Menu System.

EFT.N24.SKELS This library contains the ISPF skeletons for the eFT ISPF Menu System.

EFT.N24.MSGS This library contains the ISPF messages for the eFT ISPF Menu System.

The steps to install eFT213 are as follows:

Step 1. Receiving the Software Distribution File

Step 2. Transfer the distribution files to the z/OS system

Step 3. Tailor and Run the Installation Job

Step 4. Install the software license key

Step 5. Update your ISPF/PDF Primary Option Menu

Step 6. Automatically activate the VTAM Nodes

Step 7. Start the Multiplex Server during z/OS IPL

Step 8. Define the TCP/IP Service Names

Step 9. Place eFT into your z/OS Link List (optional)

Step 10. Tailor the Site Startup Files

Step 11. Update ISPF/PDF Command Procedure

Step 12. Customize TSO Remote Logon Files

Step 13. Authorize Multiplex Server Started Task Name

Step 14. Authorize eFT Client Proc Name

Step 15. Authorize eFT Remote Logon Proc Name

Step 16. Configure EFT for TCP Data encryption

Step 1. Receiving the Software Distribution File

The eFT software distribution format was changed beginning with Release 5.3.0. eFT213 is now distributed as a file created via the TSO XMIT (TRANSMIT) utility. NESi will distribute this file as a download via a download link. The INSTALL job will process the RECEIVE file. The .XMIT file DOES NOT have to be received by the user/customer.

We are assuming that the distribution files will be staged on an intermediate host (Windows PC or other) before they are transferred to a z/OS system.

Download the eFT213 distribution files

1. Contact technical support to request a download link for the eFT product. You may send an email to support@netex.com to request a download link.

Step 2. Transfer the distribution files to the z/OS system

Three files will be downloaded. "EFT213_N24_FTP_INST.TXT" is the ftp instructions for moving the file to the z/OS system. "EFT213_N24_INSTALL" is the actual installation job that must be configured for your system. "EFT213_N24_XMIT" is an IBM transmit file that contains multiple libraries. The install job handles receiving this file. This step may be ignored if the .INSTALL and .XMITS files are already located on the z/OS system.

At this point, you should have the eFT213 files on your PC or other desktop system. The next step will be to transfer the files to your z/OS system.

FTP transfer to z/OS from a non-z/OS system.

These instructions assume that z/OS is the **remote** system. The output filenames you use should start with the High-Level-Qualifier you plan on using for this EFT installation.

1. Connect via FTP to z/OS system.
2. Change directory to your desired high level qualifier.

   ```
   cd 'high-level-prefix'
   ```

3. If necessary change your local directory to the location the distribution files.

   ```
   lcd 'directory-name'
   ```

4. Change the FTP transfer mode to ASCII

   ascii

5. Set the required attributes for the files:

   quote site prim=6 sec=1 tracks

6. Transfer the EFT213_N24_FTP_INST.TXT file.

   ```
   put EFT213_N24_FTP_INST.TXT FTPINST
   ```

7. Set the required attributes for the files:

   ```
   quote site lrecl=80 blksize=3120 recfm=fb
   ```

8. Change the FTP transfer mode to BINARY.

   ```
   bin
   ```

9. Transfer the EFT213_N24.INSTALL file.

   ```
   put EFT213_N24.INSTALL INSTALL
   ```

10. Set these additional attributes for the .XMITS file transfer:

```
quote site prim=1000 sec=20 tracks
```

11. Transfer the EFT213_N24.XMITS file.

```
put EFT213_N24.XMITS XMITS
```

12. Quit your FTP client.

FTP transfer to z/OS from z/OS

These instructions assume that the z/OS system is the **local** system. The output filenames you use should start with the High-Level-Qualifier you plan on using for this EFT installation.

1. Connect via FTP to the system where the files are located.
2. Change directory to the location of the installation files.
3. If necessary change your local location to the desired high level prefix.

```
lcd 'high-level-prefix'
```

4. Set the required attributes for the files:

```
locsite prim=6 sec=1 tracks
```

5. Change the FTP transfer mode to ASCII

```
ascii
```

6. Transfer the EFT213_N24_FTP_INST.TXT file.

```
get EFT213_N24_FTP_INST.TXT FTPINST
```

7. Change the FTP transfer mode to BINARY.

```
bin
```

8. Set the required attributes for the files:

```
locsite lrecl=80 blksize=3120 recfm=fb
```

9. Transfer the eFT213_N24.INSTALL file.

```
get EFT213_N24.INSTALL INSTALL
```

10. Set these additional attributes for the .XMITS file transfer:

```
locsite prim=1000 sec=20 tracks
```

11. Transfer the eFT213_N24.XMITS file.

```
get EFT213_N24.XMITS XMITS
```

12. Exit out of your FTP client.

Step 3. Tailor and Run the Installation Job

The installation job will take care of "receiving" the .XMIT file. Nothing is required prior to running the install job.

The eFT213 installation job consists of four phases:

LOAD Allocates the eFT213 installation data sets and loads the data sets from the distribution.

LINK Configures the software to use the correct ROOTDIR, and ROOTDSN parameters.

EDIT Automatically tailors the eFT configuration files and sample jobs with the site specific names you provide.

COPY Copies the tailored configuration files that need to be present in a z/OS system library or to a library accessible from all eFT user sessions. The types of files copied are:

- VTAM node definitions
- Started task JCL
- TSO/E CLISTs

1. Tailor the installation job in data set EFT.N24.INSTALL. This file contains mixed case characters. Using the Caps Lock function on your keyboard will ensure dataset names have valid characters.

   Warning: DO NOT ISSUE "CHANGE xxx ALL" commands against the EFT.N24.INSTALL data set. Change the keyword values on an individual basis only.

   Change the following to meet your site requirements:

   - The JOB card(s).
   - The unit name "UNIT=(SYSALLDA,,DEFER)" on the WORK DD card. The "DEFER" keyword should be left as supplied.

2. Tailor the following installation parameters using the information you provided in section "Installation Checklist" on page 22.

   HELP Default value: NO
   Allowed values: YES NO

   The HELP parameter is used to produce a description of the eFT213 installation parameters and their usage. The value "YES" will only produce the HELP output, no other installation job phases will be executed.

   START Default value: BEGIN
   Allowed values: BEGIN LOAD LINK EDIT COPY

   The START parameter is used to determine which phase the eFT213 installation job will be started at. It can be used in conjunction with the STOP parameter to cause only a portion of the installation job to be executed.

   STOP Default value: END
   Allowed values: LOAD LINK EDIT COPY END

   The STOP parameter is used to determine which phase the eFT213 installation job will be stopped at. It can be used in conjunction with the START parameter to cause only a portion of the installation job to be executed. For example, to only execute the LINK phase, code the START and STOP parameters as:

   START(LINK)
   STOP(LINK)

   HLQ Default value: EFT.N24
   Allowed values: Any valid data set name qualifiers

The HLQ parameter is used to provide the high level qualifiers of the data set names used by the installation job. By default, the following data set names will be generated:

EFT.N24.LOAD - Program load modules

EFT.N24.LOADO - Program load modules for old DDNAMES

EFT.N24.TEXT - Configuration files and sample JCL

EFT.N24.CLIST - ISPF interface CLISTs

EFT.N24.ISPF - ISPF interface members

EFT.N24.PANELS - ISPF interface panels

EFT.N24.SKELS - ISPF interface skeletons

EFT.N24.MSGS - ISPF interface messages

Note: All the data sets defined by the HLQ parameter will be deleted and recreated by the LOAD phase.

All eFT dataset high level qualifiers (HLQ) must be the same.
All eFT dataset low level names MUST remain unchanged. ie: .text, .load, .loado, .clist, .msgs, .panels, and .skels.
If the HLQ is changed, the recommended procedure is to rerun the install with the new HLQ.
If this cannot be done, and the datasets are renamed, then all clists, all panels, all JCL for the server, all JCL for the client in batch, any JCL for TSO client MUST be modified.

Note: If symbolic VOLSERS are going to be used, this HLQ must NOT be SMS managed.

NETWORK

Default value: NETEX
Allowed values: NETEX, TCP

The NETWORK parameter is used to determine which network product eFT213 will be installed with at your site. One of the following values should be provided:

Value	Network product
NETEX	Network Executive Software H210IP/H210IPZ NetEx/IP (host based)
TCP	GSK TCP/IP/SSL

COMPRESS

Default value: NO
Allowed values: YES NO

The COMPRESS parameter is used to determine whether or not the IEBCOPY utility will be invoked to compress the eFT213 installation data sets before the data set is updated by the installation job. The COMPRESS parameter will only cause a compress of the eFT213 data sets. Other data sets used by the installation job will not be compressed. System data sets used by the COPY phase will not be compressed prior to the copies.

SYSOUT

Default value: *
Allowed values: A-Z, 0-9, *

The SYSOUT parameter is used to provide the JES SYSOUT class for utility output (IEBCOPY, etc.). The value "*" will cause the installation job MSGCLASS SYSOUT class to be used for utility output.

VOLUME Default value: None

The VOLSER to be used for all allocations if not SMS controlled.

Note: If symbolic VOLSERS are going to be used, this VOLUME must NOT be SMS managed.

UNIT Default value: SYSALLDA
Allowed values: Any valid direct access (DASD) unit name

The UNIT parameter is used to provide the z/OS unit name which will be used to allocate the eFT213 installation data sets.

OLDDDNAMES Default value: No

The standard ddnames are: "STDIN", "STDOUT" and "STDERR". If the use of the ddnames "SYSERR", "SYSIN" and "SYSPRINT" are desired, specify "YES" for this parameter. **THIS IS NOT RECOMMENDED.** This parameter is only for migration purposes and will be removed in a future release.

The OLDDDNAMES parameter is used to indicate support of the ddnames SYSOUT, SYSIN, and SYSERR in eFT Client batch JCL and command lists, as an alternative to using STDOUT, STDIN, and STDERR. This is especially useful for customers who are migrating from a version of USER-Access, and have extensive instances of USER-Access batch JCL and/or command lists that contain SYSOUT, SYSIN, and SYSERR DD statements.

ROOTDIR Default value: ' ' (use the HLQ parameter data set 'hlq.TEXT')
Allowed values: ' ' or any valid data set name

The ROOTDIR parameter is used to provide the full data set name of the Root Directory data set. The Root Directory data set is used during eFT execution to access text files such as site start up files, help files and network error messages. It is normally the "hlq.TEXT" data set name generated via the HLQ parameter. If the ROOTDIR parameter is not the same as the data set name generated by the HLQ parameter, the Root Directory data set will not be created by the installation job. It is your responsibility to correctly create the specified Root Directory data set and to copy the appropriate text files into it for later use. To use the data set name generated by the HLQ parameter as the Root Directory data set, specify this parameter as:

ROOTDIR(' ')

ASSEMBLE Default value: ASMA90
Allowed values: Any valid z/OS program name

The ASSEMBLE parameter is used to provide the name of the IBM Assembler program at your site. If you have IBM Assembler H installed, this name will usually be "IEV90". If you have the IBM High Level Assembler installed, this name will usually be "ASMA90".

ASMLOAD Default value: *
Allowed values: Any valid data set

If the Assembler program does not reside in data set SYS1.LINKLIB at your site, the ASMLOAD parameter must be added to the installation job following the ASSEMBLE parameter. Its value should be the name of the data set at your site that

contains the program specified in the ASSEMBLE parameter. The following example shows how the ASSEMBLE and ASMLOAD parameters could be specified for the IBM High Level Assembler product:

```
ASSEMBLE(ASMA90)
ASMLOAD(*)
```

LINKEDIT

Default value: IEWL
Allowed values: Any valid z/OS program name

The LINKEDIT parameter is used to provide the name of the IBM Linkage Editor or Binder program at your site. This name is usually "IEWL".

If the Linkage Editor or Binder program does not reside in data set SYS1.LINKLIB at your site, the LINKLOAD parameter must be added to the installation job following the LINKEDIT parameter. Its value should be the name of the data set at your site that contains the program specified in the LINKEDIT parameter.

SECURITY

Default value: NONE
Allowed values: NONE RACF ACF2

The SECURITY parameter is used to provide the type of security package installed at your site.

MUXTSO

Default value: TSO
Allowed values: Any valid VTAM node or ACB name

The MUXTSO parameter is used to provide the name of TSO (TCAS) at your site. Either the VTAM node name or the VTAM ACB name for TSO at your site can be used. The default value "TSO" should work for most sites.

MUXNODE

Default value: EFT001
Allowed values: Any valid VTAM node name ending in three digits

The MUXNODE parameter is used to provide the name of the first VTAM application node assigned to eFT. The EDIT phase creates a sample set of VTAM application node definitions and the COPY phase copies them into your VTAM configuration library for later activation.

MUXNODES

Default value: 10
Allowed values: 1-999

The MUXNODES parameter is used to provide the number of VTAM application nodes that will be assigned to eFT. A node is required for each concurrent eFT remote session. Nodes will be created starting with the name defined via the MUXNODE parameter and incremented by one until the MUXNODES count is reached. The default values for the MUXNODE and MUXNODES parameters will define nodes "EFT001" through "EFT010".

MUXLMODE

Default value: INTERACT
Allowed values: Any valid VTAM logon mode table entry name

The MUXLMODE parameter is used to provide the name of the VTAM logon mode table entry to be used for eFT logon to TSO/E. The entry name "INTERACT" defines an SNA 3767 (TWX) type device and is supplied by IBM in the default VTAM mode table in data set 'SYS1.VTAMLIB(ISTINCLM)'. The logon mode table entry name you provide MUST define a 3767 terminal device, not a 3270 type device. The default value "INTERACT" should work for most sites.

MUXLOGTO

Default value: 180
Allowed values: Any valid integer value

The MUXLOGTO parameter is used to provide the default time-out period, in seconds, for Multiplex Server session logon to TSO/E. The default value "180" should work for most sites.

MUXWTO

Default value: YES
Allowed values: YES NO

The MUXWTO parameter is used to determine whether or not eFT Multiplex Server session activity messages will be displayed on the z/OS system console. Session activity messages will always appear in the Multiplex Server job output, regardless of the MUXWTO parameter value.

MUXOFFER

Default value: EFT
Allowed values: Any valid network service name one to five characters long

The MUXOFFER parameter is used to provide the default network service name (service name under TCP/IP or OFFER name under NetEx) to be offered for a NON-SECURE remote user connection by the eFT Multiplex Server.

CERTDB

Default value: none

Allowed values: Valid GSKYMAN database names or RACF USERID/KEYRING values.

Determine the name of the certificate data base. This is required for secure transfers. This may be either a GSKYMAN database defined on the system, or the USERID/KEYRING if using the RACF database. Contact your security administrator for the names.

CERTPW

Default value: EFTCPWV
Allowed values: Any valid password

The CERTPW parameter specifies the read password for a GSKYMAN certificate database if data encryption is used. This can be left as a default value if you are not using encryption. You can also accept the default and define the correct value in the optional installation step 16, Configuring data security. **THIS PARAMETER MUST NOT BE CODED IF USING RACF USERID/KEYRINGS.**

CERTLB

Default value: EFTCLBV
Allowed values: 1 to 8 characters

The CERTLB parameter specifies certificate in the certificate database, if data encryption is used. This can be left as a default value if you are not using encryption. You can also accept the default and define the correct value in the optional installation step 16, Configuring data security.

SAOFFER

Default value: EFTSA
Allowed values: Any valid network service name

The SAOFFER parameter is used to provide the network service name (service name under TCP/IP or OFFER name under NetEx) to be offered for remote user connection by the eFT Standalone Server. This parameter is only used to create the Standalone Server sample JCL and should be different than the value defined via the MUXOFFER parameter.

ISPFUNIT

Default value: ' ' (none)

Allowed values: ' ' or any valid z/OS unit name

The ISPFUNIT parameter is used to provide the z/OS unit name used for allocating the eFT ISPF interface work data sets. During ISPF interface execution, each user requires three temporary work data sets of 40 kilobytes apiece.. It is recommended that this parameter specify a unit name for virtual I/O (VIO) at your site. To cause the default unit name defined in the user's TSO/E profile to be used for work data set allocation, specify this parameter as:

ISPFUNIT('')

JOBNAME Default value: EFTUSER
Allowed values: ' ' or any valid job name prefix or TSO user ID

The JOBNAME parameter is used to provide the job name prefix for the eFT sample jobs. The actual job name will be this parameter value suffixed with one additional character. To cause the sample jobs to be created without job cards, specify this parameter as:

JOBNAME('')

JOBACCT Default value: ' ' (none)
Allowed values: ' ' or any valid job accounting information

The JOBACCT parameter is used to provide job card accounting information for the eFT sample jobs.

JOBCLASS Default value: A
Allowed values: A-Z, 0-9

The JOBCLASS parameter is used to provide the job class for the eFT sample jobs.

JOBMSGCL Default value: X
Allowed values: A-Z, 0-9

The JOBMSGCL parameter is used to provide the SYSOUT message class for the eFT sample jobs.

JOBNOTFY Default value: EFTUSER
Allowed values: ' ' or any valid TSO user ID

The JOBNOTFY parameter is used to provide the TSO user ID that will be notified when an eFT sample job completes. To cause the sample job cards to be created without the NOTIFY keyword, specify this parameter as:

JOBNOTFY(' ')

JOB3 Default value: ' ' (none)
Allowed values: ' ' or any valid JCL line image

The JOB3 parameter is used to provide an additional JCL line image which follows the JOB card in the eFT sample jobs.

JOB4 Default value: ' ' (none)
Allowed values: ' ' or any valid JCL line image

The JOB4 parameter is used to provide an additional JCL line image which follows the JOB card in the eFT sample jobs.

JOB5 Default value: ' ' (none)
Allowed values: ' ' or any valid JCL line image

The JOB5 parameter is used to provide an additional JCL line image which follows the JOB card in the eFT sample jobs.

REPLACE
Default value: NO
Allowed values: YES NO

The REPLACE parameter is used to determine whether or not existing library members will be replaced in the system libraries during the COPY phase.

DISP
Default value: OLD
Allowed values: OLD SHR

The DISP parameter is used to determine whether the system libraries will be allocated for exclusive use during the COPY phase. To ensure exclusive use of the system libraries specify this parameter as:

DISP(OLD)

VTAMLST
Default value: SYS1.VTAMLST
Allowed values: ' ' or any valid data set name

The VTAMLST parameter is used to provide the name of the VTAM configuration data set at your site which will contain the eFT VTAM node definitions. The EDIT phase creates a sample set of VTAM application node definitions and the COPY phase copies them into your VTAM configuration library for later activation. To bypass the copy of the node definitions, specify this parameter as:

VTAMLST(' ')

VTAMNODE
Default value: EFTVAPPL
Allowed values: Any valid VTAM major node name

The VTAMNODE parameter is used to provide the name of the VTAM major node assigned to eFT. This parameter will also be the member name in the data set defined via the VTAMLST parameter.

PROCLIB
Default value: SYS1.PROCLIB
Allowed values: ' ' or any valid data set name

The PROCLIB parameter is used to provide the name of the JCL procedure library data set at your site which will contain the JCL needed to execute the eFT Multiplex Server as a started task. The EDIT phase creates the started task JCL procedure and the COPY phase copies it into your system JCL procedure library for later activation. To bypass the copy of the JCL procedure, specify this parameter as:

PROCLIB(' ')

PROCNAME
Default value: EFTMSERV
Allowed values: Any valid JCL procedure name

The PROCNAME parameter is used to provide the name for the z/OS started task used to run the eFT Multiplex Server. This parameter will also be the member name in the data set defined via the PROCLIB parameter.

CMDPROC
Default value: SYS1.CMDPROC
Allowed values: ' ' or any valid data set name

The CMDPROC parameter is used to provide the name of a CLIST library which can be accessed by all TSO users at your site. The eFT CLISTs needed to run the eFT Client program and for the eFT ISPF interface will be placed into this data set during the COPY phase. All CLIST names will begin with the three characters “EFT”, except the CLIST name defined via the CMDNAME parameter. To bypass the copy of the CLISTs, specify this parameter as:

CMDPROC(' ')

CMDNAME Default value: EFT
Allowed values: Any valid TSO/E command name

The CMDNAME parameter is used to provide the command name used by TSO/E users to start the eFT Client program. This parameter will also be the member name in the data set defined via the CMDPROC parameter. It is recommended that this name be left as “EFT” so that the eFT TSO/E command name matches the eFT documentation.

ISPPLIB Default value: None

Allowed values: ' ' or any valid data set name

The ISPPLIB parameter is used to provide the name of an ISPF panel library which can be accessed by all TSO users at your site. The panels needed for the eFT ISPF interface will be placed into this data set during the COPY phase. All panel names will begin with the characters "NUAI" or “EFT”.

ISPSLIB Default value: None

Allowed values: ' ' or any valid data set name

The ISPSLIB parameter is used to provide the name of the ISPF skeleton library which can be accessed by all TSO users at your site. The skeletons needed for the eFT ISPF interface will be placed into this data set during the COPY phase. All skeleton names will begin with the characters "NUAI" or “EFT”.

ISPMLIB Default value: None

Allowed values: ' ' or any valid data set name

The ISPMLIB parameter is used to provide the name of the ISPF message library which can be accessed by all TSO users at your site. The messages needed for the eFT ISPF interface will be placed into this data set during the COPY phase. All message names will begin with the characters "NUAI" or “EFT”.

3. Submit the job for execution and verify all of the steps complete with a condition code of zero. You may receive a condition code of 4, if you bypass the copy of members into installation dataset by using dataset names of ‘’ for PROCLIB, CMDPROC, VTAMLST etc. It is then up to the user to update the system datasets.

Step 4. Install the software license key

If you have not already received a key, contact NetEx Software customer support at support@netex.com and request a software key.

If your site requires secure transfers, a new feature code is added to the license key. This is a separately chargeable feature for the TCP version of the product only. Encryption is not supported in the NETEX version.

Support will require the CPU serial number for the z/OS system. This information is found by executing the z/OS command “D M=CPU”. E-mailing the output from this command to customer support is the preferred method.

Each NetEx Software product that has integrated the License Verification Software facility now contains a product configuration file and a license key file. The NetEx/eFT product includes these files in its installation distribution file set. During installation, the files PRODCONF and LIC are installed in the EFT.N24.TEXT data set.

The Product License Key has an associated expiration date; therefore a new key must be obtained and installed before the prior key’s expiration in order to prevent interruptions in the product’s operation.

Note: Customers using multiple NESi software products (e.g., NetEx, BFX, etc.) may choose to store all of their software license keys in a centralized keys file. In those configurations, customers may choose to edit the "LICPATH" parameter in the EFT.N24.TEXT(PRODCONF) file to refer to the desired license key file.

The PRODCONF DD/file

The PRODCONF file points to the location of the LIC file which contains the actual software license key. The default PRODCONF file shipped with NetEx/eFT contains the following information:

```
* COMMENT 1
LICPATH  //DSN:EFT213.N24.TEXT(LIC)
* LICPATH  //DDN:LICENSE
* COMMENT 2
```

An asterisk 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. Customer support will reply with a software key that should be entered into the file LIC located in EFT.N24.TEXT.

The LIC file

In a default eFT installation, the License Verification Software facility looks for the license key in a file called LIC which can be found in the EFT.N24.TEXT data set. The location of this file may be changed by modifying the value of the LICPATH parameter in the PRODCONF file.

The systems programmer installing eFT213 must edit this file to add a new encrypted software key each time a key is obtained from NetEx Software for the eFT213 product.

The LIC file may contain multiple keys for a variety of NESi software products. However, if there are multiple eFT keys in the LIC file (for instance, due to changes in eFT features licensed), the key that relates to those changes must be the FIRST uncommented eFT key located in that file.

The LIC file installed with the distribution contains the following information:

```
* EFT213 LICENSE
PUT LICENSE KEY HERE
* THE END
```

A leading asterisk character ("*") on a line denotes a comment line.

The software license key must appear on an uncommented line by itself without any leading or trailing spaces or characters.

Step 5. Update your ISPF/PDF Primary Option Menu

Add EFT to your ISPF/PDF Primary Option Menu or other ISPF option menu.

1. The supplied panel (EFT@PRIM) in the dataset EFT.N24.PANELS is an example of how to add EFT to your ISPF/PDF Primary Option Menu. (EFT@PRIM was an updated copy of ISR@PRIM.)

   Line 15,

   ```
   % EFT +Netex EFT   - EFT ISPF Menu System
   ```

   line 34,

   ```
   &EFTIOPT = .TRAIL
   ```

   and lines 48-50

```
EFT,'CMD(%EFTUSER MENU EFTIOPT(''&EFTIOPT'') +
     SCR(''''''EFT.N24.TEXT(EFTIISPF)'''''')) +
     NOCHECK NEWAPPL(NUAI)'
```

were added to the default ISPF/PDF Primary Option Menu provided by IBM (ISR@PRIM). Add the five new lines to your ISPF/PDF Primary Option Menu ISR@PRIM (or other ISPF option menu), being careful to ensure that the lines are added in the same relative ISPF processing order.

2. Ensure the "SCR" keyword (line 49 of EFT@PRIM) points to the data set containing the EFT ISPF start up script as supplied in the dataset EFT.N24.TEXT. Be careful not to change the number of apostrophes surrounding the data set name.

If you changed your ISPF/PDF Primary Option Menu, be sure to test it before replacing your current Primary Option Menu. If the new Primary Option Menu has an error, ISPF or ISPF/PDF may become unusable until you fix the error using a non-ISPF utility program. Refer to the appropriate ISPF and ISPF/PDF publications for additional information on how to change and test ISPF menus.

Step 6. Automatically activate the VTAM Nodes

1. If the eFT VTAM nodes are to be automatically activated during VTAM start up, you should add the VTAM major node name EFTVAPPL or the name you provided via the VTAMNODE(...) parameter in the installation job, to your VTAM configuration list in data set SYS1.VTAMLST(ATCCON00) or the equivalent data set at your site.

2. An alternative method to activate the VTAM nodes is to issue the following command as part of your z/OS IPL procedure, after VTAM initialization has completed:

```
V NET,ACT,ID=EFTVAPPL
```

Step 7. Start the Multiplex Server during z/OS IPL

1. The eFT Multiplex Server can be executed as either a batch job or a z/OS started task. It is suggested that the Multiplex Server be started at z/OS IPL time, either automatically or as part of the computer operations IPL procedure. Remember that the eFT VTAM nodes should be active before the Multiplex Server is started.

2. Set the Multiplex Server to a relatively high dispatching priority on your z/OS system, usually just below VTAM, NetEx, and/or TCP/IP. Multiplex Server resource utilization is minimal since z/OS users executing the eFT Client program do not interface with the Multiplex Server. Also, most remote user eFT activity (including file transfer) occurs under and is reported against the remote user's TSO/E session while executing the Helper program.

Step 8. Define the TCP/IP Service Names

If you are installing eFT213 with a network type of "TCP" you must complete this step. For a network type of "NETEX", you should skip this step.

1. If you are installing with the IBM Communications Server network product, you must define the service names "EFT" and "eft" (or the service name you provided via the MUXOFFER(...) parameter in the installation job), to use the default eFT well known port number of 6900 in data set TCPIP.ETC.SERVICES. Note that IBM Communications Server service names are case sensitive and both the upper case and lower case names should be equated to the well-known port number. The following line is an example of how to define port number 6900:

```
eft      6900/tcp          # EFT213 Multiplex Server
EFT      6900/tcp          # EFT213 Multiplex Server
```

You may also want to define well known port numbers for any Standalone Server service names you have selected. Refer to the IBM Communications Server publications for additional information on how to define service names.

```
eftsa     6901/tcp          # EFT213 Standalone Server
EFTSA     6901/tcp          # EFT213 Standalone Server
```

2. Different port numbers can be used other than 6900, 6910 and 6901, but it is a requirement that ALL TCP/IP hosts in the network have the same well known port number defined for eFT services.

Step 9. Place eFT into your z/OS Link List (optional)

Optionally make the eFT213 load modules available to all users and jobs in your system. This step is **no longer recommended** since all allocations for eFT are done via clists except for the server JCL.

You can either:

1. Add the eFT213 load module data set name defined via the LOAD(...) parameter in the installation job, to your z/OS link list concatenation as defined in data set SYS1.PARMLIB(LNKLST00).
2. Copy all the load modules from the data set defined via the LOAD(...) parameter in the installation job, to data set SYS1.LINKLIB or other existing data set in your z/OS link list concatenation.
3. Add an NUALIB DD statement (or allocation for TSO) where appropriate. **This is the default**.

Step 10. Tailor the Site Startup Files

Additional information may be found in the eFT Software Reference Manual; "IBM/zOS Local User's Guide.

1. The *HLQ*.TEXT(SCLIENT) member is for all eft users. Each user can supplement this member by creating a *PREFIX*.CLIENT.UA file with additional commands.
2. The *HLQ*.TEXT(SSERVER) member is for all remote logons to the eFT Server. Each user can supplement this member by creating a *PREFIX*.SERVER.UA file with additional commands.

   The Server site start up file is passed to and executed by the remote Client program as part of CONNECT command processing. It is passed by both the Multiplex Server (via the Helper program) and by the Standalone Server (directly).

Step 11. Update ISPF/PDF Command Procedure

Update your ISPF/PDF command procedure that gets executed during logon processing (usually specified as a parameter on the TSO logon proc), to include the eFT CMDPROC library (e.g., 'EFT.N24.CMDPROC') in the SYSPROC allocation. Or, if a new TSO proc is going to be used for eFT client logons, be sure the ISPF/PDF command procedure that is used with the new eFT client logon proc includes the eFT CMDPROC library in the SYSPROC allocation.

If site-defined ISPF libraries are used to contain the eFT ISPF panels, skeletons, and messages, then add the site-defined panel library to the ISPPLIB allocation; add the site-defined skeleton library to the ISPSLIB allocation; and add the site-defined messages library to the ISPMLIB allocation.

Step 12. Customize TSO Remote Logon Files

Review the TEXT library (e.g. 'EFT.N24.TEXT') member EFTMCONF.

The only service defined at installation time is
EFT for non-secure connections

For each service support, review the following parameters:

USERNAME, PASSWORD, ACCOUNT, and PROFILE(PROCNAME), PORT_MIN, PORT_MAX. These values get used during TSO Remote Login processing, on behalf of an eFT client connecting to the eFT Multiplex Server. The connecting eFT client must specify values for each of these parameters that do not contain a default in the EFTMCONF file.

The USERNAME and PASSWORD identify the connecting user and are used to establish the TSO session. ACCOUNT specifies the ACCOUNT number used when the TSO session is established. PROFILE identifies the TSO logon proc used for the TSO session

By default, the remote login will take place and then EFTALOCM clist will be invoked to allocate the required files and then call NUAHELPR.

If desired, customize the EFTMCONF member located in the TEXT library (e.g. 'EFT.N24.TEXT') to include default values for PORT_MIN and PORT_MAX. These parameters specify a range of z/OS ports that will be used for subsequent eFT data connections for the remote client. If these parameters are not changed or set to zero (0), the systems ephemeral port range will be used. Specify values for these parameters that satisfy your site security requirements.

Step 13. Authorize Multiplex Server Started Task Name

If you use RACF (or another security product) it may be necessary to define the Multiplex Server Started Task name to the security system in order to identify it as an authorized Started Task. Whether this step is required or not depends on the level of security deployed on your system. Consult with the System Administrator responsible for the z/OS system to determine what is required for this step.

Step 14. Authorize eFT Client Proc Name

If you use RACF (or another security product), and you defined a new TSO proc for the eFT client logon (Step 9), it may be necessary to define the eFT client logon proc name to the security system, in order to identify it as an authorized TSO proc. Whether this step is required or not depends on the level of security deployed on your system. Consult with the System Administrator responsible for the z/OS system to determine what is required for this step.

Step 15. Authorize eFT Remote Logon Proc Name

If you use RACF (or another security product), and you defined a new TSO proc for the eFT remote logon (Step 10), it may be necessary to define the eFT remote logon proc name to the security system, in order to identify it as an authorized TSO proc. Whether this step is required or not depends on the level of security deployed on your system. Consult with the System Administrator responsible for the z/OS system to determine what is required for this step.

This completes the eFT213 installation procedure. Please review "Installation Notes" on page 9 again, and then proceed with the "Installation Verification Procedure" on page 38.

Step 16. Configuring TCPIP eFT213 for Data Encryption (OPTIONAL)

This is a separately chargeable feature available in the TCP/IP version of the product. It is recommended you validate the software in your environment in a non-secure mode before implementing a data secure mode.

Users may wish to run eFT in one of three ways.

1. As it is installed, eFT will run in a NON-SECURED mode. All TCP traffic will be transmitted in clear text.

2. The user may wish to upgrade this service to SECURE mode only. All data and user protocol will be encrypted before entering the network.
3. The user may wish to offer both a SECURE mode and a NON-SECURED mode

For NON-SECURED mode:

No additional work is required. This is the default installation mode.

FOR SECURE mode only:

For the MUXSERVER:

Edit the HLQ.TEXT(EFTMCONF) member find the "SECURE CONNECTIONS" section.

1. Uncomment the line SECURE ON
2. Uncomment the line FIPSLVL 0
    a. 0 is the least secure. The range is 0-3.
    b. See the IBM documentation for "gsk-fips_state_set" for the complete requirements for each level.
3. Uncomment the line CERTDB. This line should reflect either the name of your GSKYMAN certificate database, or a RACF USEID/KEYRING on your z/OS system. If it shows "EFTCDBV' the name of the certificate data base was not supplied during the install process. You may change the EFTCDBV to the name of your file. In some cases, this maybe a unix style name, so case is sensitive.
4. Uncomment the line CERTPW. This line should reflect the read password to the GSKYMAN certificate database. If it shows EFTCPW, the password was not supplied at installation time. You may change EFTCPWV to the read password. This is case sensitive. **THIS MUST NOT BE CODED IF USING RACF USERID/KEYRINGS.**
5. Uncomment the line CERTLB. This line should reflect the name of the certificate to use. If this shows EFTCLBV, the certificate name was not supplied at the installation time. You may change the value to reflect the certificate name to use.
6. Uncomment the line SSLPROTOCOL and set the value as desired. The – means to remove this protocol. Protocols supported are TLSv1, TLSv1_1 and TLSv1_2. SSLV2 and SSLV3 are no longer supported.
7. To restrict encryption to a set of ciphers, uncomment the line SSLCIPHERS and set the value as desired. The four digit SSL CIPHERS are defined in the " z/OS Cryptographic Services System SSL Programming".

The muxserver or the standalone server must be restarted for these values to be in effect.

For clients on this MVS system wishing to connect to a SECURE mode server, all the security information must be supplied. This information may be specified in the connect environment, or may be included on the connect statement. A sample showing this on the connect statement is included in the *HLQ*.TEXT(SCLIENT) member. The SCLIENT member is the site wide startup script run when a client is started on this z/OS system. After the Welcome message is written an alias is defined for SECCON. This alias will prompt the user for a host name to connect to, the userid to use and the password. It will then provide a secure connection to that host. The –serv eftds will attempt to connect to that service on the Host system. You may have to change eftds for your configuration. –secure requires a secure data connection. –certdb is the name of the GSKYMAN certificate database that will be used, or a RACF USERID/KEYRING. –certpw is the read password for the GSKYMAN database (**THIS MUST NOT BE CODED IF USING RACF USERID/KEYRINGS)**, and –certlb is the name of the certificate to use. In most cases, these will match the values used in the EFTMCONF file, as both the client and Mux server are running on the same system. If connecting to a different host, these same values can be used, if certificates are properly configured.

FOR SECURE and NON_SECURE mode:

For the MUXSERVER

edit the HLQ.TEXT(EFTMCONF) member.

1. Find the comment line "*SERV KEYWORD VALUE"
2. Starting with the line you just found, copy all lines to the end of the file after the last statement in the file.
3. Find the second comment line "*SERV KEYWORD VALUE"
4. Change EFT to the name of the service you wish to be secured
5. Update TCPIP.ETC.SERVICES to reflect the new service
6. In the second "SECURE CONNECTIONS" section.
7. Uncomment the line SECURE ON
8. Uncomment the line CERTDB. This line should reflect the name of your GSKYMAN certificate database on your z/OS system or a RACF USERID/KEYRING if you are using RACF. If is shows "EFTCDBV' the name of the certificate data base was not supplied during the install process. You may change the EFTCDBV to the name of your file. In some cases, this maybe a unix style name, so case is sensitive.
9. Uncomment the line CERTPW. This line should reflect the read password to the GSKYMAN certificate database. **IT MUST NOT BE CODED IF YOU ARE USING RACF USERID/KEYRINGS.** If it shows EFTCPW, the password was not supplied at installation time. You may change EFTCPWV to the read password. This is case sensitive.
10. Uncomment the line CERTLB. This line should reflect the name of the certificate to use. If this shows EFTCLBV, the certificate name was not supplied at the installation time.
11. Uncomment the line SSLPROTOCOL and set the value as desired. The – means to remove this protocol. Protocols supported are TLSv1, TLSv1_1 and TLSv1_2. SSLV2 and SSLV3 are no longer supported.
12. To restrict encryption to a set of ciphers, uncomment the line SSLCIPHERS and set the value as desired. The four digit SSL CIPHERS are defined in the " z/OS Cryptographic Services System SSL Programming".

The muxserver or the standalone server must be restarted for these values to be in effect. The MUXSERVER will now have two services offered. One is non-secure, and the clients cannot use this service to connect to securely (-secure), and the second service which is secured. The client must use the –secure parameter.

For clients connecting to the system securely, they must include all the security parameters. See the preceding statement for clients in the SECURE ONLY section. For non-secure connections, they must not code the –SECURE parameter.

1. Issue the eFT command for a secure connection the output should be the same as above:

```
EFT> seccon
Hostname? ZOS
Username? userid
Password? xxxxx
```

2. Issue the eFT command:

```
EFT> SHOW HOST
```

eFT should produce output similar to the following:

```
EFT:
EFT: active --> (1) Host=zos Secure=on  User=userid
EFT:
```

3. Issue the eFT command:

```
EFT> SHOW REMOTE
```

eFT should produce output similar to the following:

10.1.5.64> show remote
eFT:
eFT: * BLOCKsize 16384
eFT: * COPYRight ..... COPYRIGHT (c) 1999-2021 - Network Executive Software, Inc. Mpls. MN
eFT: DIRectory ..... *prefix*
eFT: * GATEway .....
eFT: HOMEdir ..... *prefix*
eFT: * HOST 10.1.5.64
eFT: * HOSTCODE ..... EBCDIC
eFT: * HOSTENV ..... TSO FOREGROUND
eFT: * HOSTOS ..... z/OS 2.3
eFT: * HOSTTYPE ..... MVS
eFT: * LicExp 20191002
eFT: * LicKey DSEJ-YAC2-AD7Q-CAOT-QCYJ-RH36-C27N-VPV7
eFT: * LicNotOper 20191231
eFT: * LicProto ..... NTX IP SSL
eFT: * PID 0XF9C1008D92D8
eFT: PREFix ..... MVS:
eFT: * PRODuct EFT213
eFT: QUIet ..... off
eFT: * ROOTdir EFT0550.TEXT
eFT: * SECure ..... ON
eFT: * SERvice ..... efts
eFT: * SSLCipher 0035
eFT: * SSLProto TLSV1.2
eFT: * STATus .....
eFT: * TRANSlate ..... Network
eFT: TSOPREfix ..... *userid*
eFT: * USERname *BROWND1*
eFT: * VERsion 5.5.0-9621 N24
eFT:
eFT: * Informational qualifier (cannot be modified).
eFT:

The SSLCipher codes are defined in Appendix C of the "IBM "Cryptographic Services System Secure Sockets layer Programming" manual SC14-7495-00.

Post-Installation Note (TEXTLIB DD statement):

The TEXTLIB DD statement should point to the location of the EFT.N24.TEXT file if it will be different than the installation configured dataset. This makes it possible to *share* a set of install libraries on multiple systems with different catalog aliases, or facilitates copying one set of libraries for use on different systems.

Installation Verification Procedure

Perform the following Installation Verification Procedure (IVP) to ensure eFT213 is functioning correctly at your site. This IVP assumes you have completed all steps required to fully install eFT213. If you have customized eFT above and beyond the supplied installation procedure, the output produced during the IVP will reflect those changes.

The steps to verify the eFT installation are as follows:

Step 1. Test the Client

Step 2. Start the Multiplex Server

Step 3. Test the Multiplex Server

Step 4. Stop the Multiplex Server

Step 1. Test the Client

1. Log on to TSO/E according to your existing site procedures.
2. Issue one of the following TSO/E commands:

   ```
   %EFT
   %EFTUSER
   ```

   The eFT Client program will initialize and produce output similar to the following:

   ```
   %EFT - EFT starting
   EFT>
   ```

3. Issue the eFT command:

   ```
   EFT> HELP MVS
   ```

   eFT should produce output similar to the following:

   ```
   EFT: This level of help is intended to give you a better
   EFT: understanding of the IBM/ZOS implementation of the
   EFT: EFT product.
   EFT:
   EFT: Additional help is available on the following subtopics:
   EFT:
   EFT: CONNecting  CONVersion   CREating_DS    DIRectory
   EFT: DS_org      Filespecs    HOST_commands  RECformats
   EFT: MODes       WILDcarding  DEST_wildcard
   ```

   If the above output was not produced, ensure the Root Directory data set name was supplied correctly during eFT213 installation and that the help text files exist in the Root Directory data set.

4. Issue the eFT command:

   ```
   EFT> LOCAL DIRECTORY
   ```

   A listing of the data sets with your local TSO/E prefix should be produced similar to one produced using the TSO/E LISTCAT command.

5. If eFT is installed on other hosts in your network, you can try and establish connections to a remote host at this time according to the eFT User Guide.

6. Issue the eFT command:

```
EFT> QUIT
```

eFT should produce output similar to the following:

```
%EFT - EFT complete - Code(0)
READY
```

If all the above steps completed successfully, the Client side of eFT is installed correctly.

Step 2. Start the Multiplex Server

1. If the eFT VTAM application nodes are not active, issue the VTAM console command:

```
V NET,ACT,ID=EFTVAPPL
```

Where eFTVAPPL is the VTAM major node name provided via the VTAMNODE(...) parameter in the installation job.

2. If you have decided to run the Multiplex Server as a batch job, submit the Multiplex Server execution JCL in the dataset EFT.N24.TEXT.

If you have decided to run the Multiplex Server as a started task, issue the z/OS console command:

```
START EFTMSERV
```

Where EFTMSERV is the Multiplex Server JCL procedure name provided via the PROCNAME(...) parameter in the installation job.

The Multiplex Server log (SYSPRINT and EFTMLOG DD statements) should contain output similar to the following, preceded by date/time information:

```
NUAVTAM  NUA2000I Version 5.5 N24 Compiled 2021 Sept 24
MSERVER  MServer:Input=DD:EFTMCONF.
MSERVER  .
MSERVER  Multiplex Server version EFT5.5  started.
MSERVER  COPYRIGHT(c)1999-2021-Network Executive Software, Inc. Mpls. MN.
MSERVER  Trace flag settings: .
MSERVER  LicKey=C3JY-YAC2-AAAV-JWC2-7HOE-W3PD.
MSERVER  LicNotOperational=20151231.
MSERVER  LicExpiration=20191002.
MSERVER  Trace flag settings: 0123456789ABCDEF.
```

If the above output was produced, the Multiplex Server has started correctly. If not, ensure the Multiplex Server execution parameters and VTAM configuration parameters were tailored correctly during installation.

Step 3. Test the Multiplex Server

4. Invoke the eFT Client program as described in “Step 1. Test the Client” on page 38 or invoke an eFT Client program on a remote host. If you invoke eFT on a remote host, the following commands will be issued on that host.

5. Issue the eFT command for a non-secure connection:

```
EFT> CONNECT zos userid password  -secure no
```

Where “zos” is your network host name for this z/OS system, “userid” is a valid TSO/E user ID for this z/OS system, and password is a valid “password” for the user ID. If you have RACF installed, you may also need to supply a valid account number and logon procedure name, for example:

```
EFT> CONNECT zos userid password –secure no -ACCOUNT nnnn -PROFILE ppppp
```

If you have a TSO/E logon procedure similar to the one provided with TSO/E, eFT should produce output similar to the following:

```
EFT: Connected to service 'EFT' on host 'zos'.
============================================================
userid LOGON IN PROGRESS AT 16:48:57 ON APRIL 2, 2012
NO BROADCAST MESSAGES
READY
============================================================
EFT: Logged in as user 'userid'.
```

If your CONNECT command did not produce any immediate output, be patient, the CONNECT command will time out after about 3 minutes (the default time out interval), issue error messages, and display any TSO/E logon messages produced.

Any problems encountered will most likely be related to the CONNECT command parameters, the Multiplex Server execution parameters, or your z/OS security product. For more information refer to the section “The Multiplex Server and TSO/E Logon Processing” on page 43.

You must have a successful CONNECT command before continuing with this IVP.

6. Issue the eFT command:

   ```
   EFT> SHOW HOST
   ```

   eFT should produce output similar to the following:

   ```
   EFT:
   EFT: active --> (1) Host=zos Secure=off  User=userid
   EFT:
   ```

7. Issue the eFT command:

   ```
   EFT> SHOW REMOTE
   ```

   eFT should produce output similar to the following:

   ```
   eFT:
   eFT: * BLOCKsize ......... 16384
   eFT: * COPYRight ......... COPYRIGHT (c) 1999-2021 - Network Executive Soft-
   ware, Inc.  Mpls. MN
   eFT:   DIRectory ......... prefix
   eFT: * GATEway ...........
   eFT:   HOMEdir ........... prefix
   eFT: * HOST .............. zos
   eFT: * HOSTCODE .......... EBCDIC
   eFT: * HOSTENV ........... TSO FOREGROUND
   eFT: * HOSTOS ............ z/OS 2.3
   eFT: * HOSTTYPE .......... MVS
   eFT: * LicExp ............ 20191002
   eFT: * LicKey ............ DSEJ-YAC2-AD7Q-CAOT-QCYJ-RH36-C27N-VPV7
   eFT: * LicNotOper ........ 20191231
   eFT: * LicProto .......... NTX IP SSL
   eFT: * PID ............... 0XF9C1008D92D8
   eFT:   PREFix ............ MVS:
   eFT: * PRODuct ........... EFT213
   eFT:   QUIet ............. off
   eFT: * ROOTdir ........... EFT0550.TEXT
   eFT: * SECure ............ OFF
   eFT: * SERvice ........... 6914
   eFT: * SSLCipher .........
   eFT: * SSLProto ..........
   eFT: * STATus ............
   eFT: * TRANSlate ......... Network
   ```

```
eFT:   TSOPREfix ......... prefix
eFT: * USERname .......... userid
eFT: * VERsion ........... 5.5.0-9621 N24
eFT:
eFT: * Informational qualifier (cannot be modified).
eFT:
```

8. Terminate the connection to the host.
   a. disc
   b. bye

9. Issue the eFT command:
   ```
   EFT> REMOTE DIRECTORY
   ```
   A listing of the data sets with your remote TSO/E prefix should be produced similar to one produced using the TSO/E LISTCAT command.

10. Issue the eFT command:
    ```
    EFT> RECEIVE '{rootdir:remote}(USERHELP)' TEST.MVS -CREATE REPLACE
    ```
    This will initiate an eFT file transfer of the eFT help text. eFT should produce output similar to the following:
    ```
    EFT: Source                      Destination                 Size
    EFT: ------------------------   ------------------------     -------
    EFT: EFT.N24.TEXT(EFTHELP)       prefix.TEST.MVS             60155
    ```
    The file names and file size may be different than shown above. This is not a problem and the output may change depending upon the remote host operating system you are using and the size of the eFT help file.

11. You may want to delete the destination file at this point.

    If you are running the client program on a z/OS host, issue the eFT command:
    ```
    EFT> LOCAL DELETE TEST.MVS
    ```
    eFT should produce output similar to the following:
    ```
    IDC0550I ENTRY (A) prefix.TEST.MVS DELETED
    ```
    If you are running the client program on a remote host, refer to the eFT User Guide for the remote host you are using for that host's DELETE command syntax and output.

12. Issue the eFT command:
    ```
    EFT> QUIT
    ```
    If you are running the client program on a z/OS host, the eFT Client program should produce output similar to the following:
    ```
    %EFT - EFT complete - Code(0)
    READY
    ```
    If you are running the client program on a remote host, refer the eFT User Guide for the remote host you are using for that host's output produced by the QUIT command.

    If all the above steps completed successfully, the Multiplex Server side of eFT213 is installed correctly.

Step 4. Stop the Multiplex Server

To stop the Multiplex Server, issue the z/OS console command:

```
STOP EFTMSERV
```

Where EFTMSERV is the name of the Multiplex Server job you submitted or the Multiplex Server started task JCL procedure name. The Multiplex Server should end within about 30 seconds of acknowledging the STOP command.

This completes the eFT213 Installation Verification Procedure.

Post Installation Considerations

The Multiplex Server and TSO/E Logon Processing

The eFT213 Multiplex Server is designed to support the TSO/E logon procedure at your site. Your site specific logon procedure is described to the Multiplex Server by customizing logon control keywords in the Multiplex Server execution parameters. These keywords control the initial LOGON command sent to TSO/E and examine each logon output message to see if any action is needed.

eFT does not support an “interactive” logon, so replies to logon prompts or messages must be supplied on the remote CONNECT command and/or the Multiplex Server execution parameters. Refer to the section “Connecting to a z/OS host” in the eFT User Guide for more information on the CONNECT command.

Logon keywords are supplied in the Multiplex Server execution parameters in the dataset EFT.N24.TEXT. All keywords except “LOGON” are suffixed with a number from 1 to 50 allowing multiple occurrences of that keyword. The suffixes MUST be assigned in ascending order and are unrelated except for the “PROMPTn” and “RESPONSEn”. The following is a brief description of each keyword:

LOGON	Format of the LOGON command sent to TSO/E
PROMPTn	Text that flags an output message as a prompt
RESPONSEn	Text that is supplied as a response to a prompt
SUCCESSn	Text that indicates the logon has successfully completed
FAILUREn	Text that indicates the logon has failed
SUPPRESSn	Text that causes the logon message not to be displayed

The TSO/E LOGON command format is controlled by the “LOGON” keyword. String substitution is performed on the text using the parameters supplied on the CONNECT command. The parameters to be substituted are enclosed in curly braces “{}” and can be one of the following values:

USERNAME	The CONNECT user name
PASSWORD	The CONNECT password
ACCOUNT	The account number supplied with the -ACCOUNT qualifier
COMMAND	The command name supplied with the -COMMAND qualifier
PROFILE	The profile name supplied with the -PROFILE qualifier
PROJECT	The project number supplied with the -PROJECT qualifier
SCRIPT	The script name supplied with the -SCRIPT qualifier
SECONDARY	The secondary password supplied with the -SECONDARY qualifier
1,2,3...n	Positional parameters following the CONNECT password

The default “LOGON” keyword shown below is supplied in the Multiplex Server execution parameters and passes the CONNECT command user name and CONNECT command password separated by a slash ('/'), followed by any text supplied in the CONNECT command positional parameter 1.

```
LOGON {USERNAME}/{PASSWORD} {1}
```

The “LOGON” text can be modified to include site specific parameters. The following “LOGON” text would disable TSO/E mail messages:

```
LOGON {USERNAME}/{PASSWORD} NOMAIL {1}
```

After the TSO/E LOGON command is issued, the text from the “PROMPTn”, “SUCCESSn”, “FAILUREn” and “SUPPRESSn” keywords is compared to each logon output message. If a match is found, the processing for the keyword is performed. A leading ‘<’ compares the text to the beginning of the logon message and a trailing ‘>’ compares the text to the end of the message. Text without a leading ‘<’ and trailing ‘>’ is searched for anywhere in the message.

“PROMPTn” and “RESPONSEn” are paired keywords, where “RESPONSE1” is the reply for the “PROMPT1” logon message. String substitution is performed on “RESPONSEn” keywords using the same CONNECT parameters given for the “LOGON” keyword above. If no “RESPONSEn” keyword is supplied for a “PROMPTn” keyword, a null line (just the ENTER or RETURN key) is replied to the prompt. Remember that “PROMPTn” keywords are case sensitive.

The logon message:

```
IKJ56415I CURRENT PASSWORD HAS EXPIRED - PLEASE ENTER NEW PASSWORD
```

could be tested for with the “PROMPTn” keyword of:

```
PROMPT1 PLEASE ENTER NEW PASSWORD
```

and replied to with the “RESPONSEn” keyword of

```
RESPONSE1 {SECONDARY}
```

The response text will be appended to the prompt message for display to the remote user. In the case where a response consists of a password, this may not be acceptable and use of the “SUPPRESSn” keyword (described below) may be necessary.

Once a “PROMPTn” keyword has been matched, its text is no longer compared against subsequent logon messages. This prevents eFT from supplying incorrect “RESPONSEn” text to a repeating logon prompt. The same text may be specified for another “PROMPTn” keyword when the same logon prompt appears again, along with new “RESPONSEn” text.

If your site does not support anything but the “vanilla” TSO/E logon, you may not need to reply to any prompt requests. In this case the above logon message would be considered a logon problem and a “FAILUREn” keyword could instead be specified as:

```
FAILURE1 PLEASE ENTER NEW PASSWORD
```

Any “FAILUREn” match causes the remote CONNECT command to terminate immediately with an error message and the TSO/E session to be terminated.

The TSO/E “READY” message normally indicates the TSO/E logon has completed successfully. The following “SUCCESSn” keyword tests this case:

```
SUCCESS1 <READY
```

Once a “SUCCESSn” keyword has been matched, no further logon keywords are processed, no further messages are displayed to the remote user, and CONNECT command processing continues.

You may want to suppress additional logon messages. For example some TSO/E logon procedures invoke the ISPF product. Since eFT does not support “full screen” products for remote users, ISPF may issue the message:

```
INVALID SCREEN SIZE, ONLY 24X80, 32X80, 43X80, 27X132, 62X160 ALLOWED
```

You could suppress display of this message for the remote user by supplying the following “SUPPRESSn” keyword:

```
SUPPRESS1 INVALID SCREEN SIZE
```

“SUPPRESSn” keywords can also be used to suppress “PROMPTn” messages that have a “RESPONSEn” keyword that supplies a password. For the “PROMPT1” example above, we could add a “SUPPRESSn” keyword of:

```
SUPPRESS2 PLEASE ENTER NEW PASSWORD
```

z/OS security products such as RACF, CA-ACF2, etc. may significantly alter the TSO/E logon process. The supplied Multiplex Server execution parameters may include suggested logon keywords for your security product. If an example is found that matches your security product, change the default logon

keywords to comment lines (or delete them) and remove the comment character ('*' in column one) from the alternate definitions. The default logon keywords for your security product may also require changes.

The new keywords will take effect the next time the Multiplex Server is started.

Starting and Stopping the Multiplex Server

The following procedure describes how to start and stop the eFT213 Multiplex Server. This procedure uses the data set names supplied on the distribution.

Most sites will not allow an end user to start the Multiplex Server. The Multiplex Server will usually be started by computer operations as part of their z/OS IPL procedure.

Starting the Multiplex Server

1. If the eFT VTAM application nodes are not active, issue the VTAM console command:

   ```
   V NET,ACT,ID=EFTVAPPL
   ```

   Where EFTVAPPL is the VTAM major node name provided via the VTAMNODE(...) parameter in the installation job.

2. If you have decided to run the Multiplex Server as a batch job, submit the Multiplex Server execution JCL in the dataset EFT.N24.TEXT.

   If you have decided to run the Multiplex Server as a started task, issue the z/OS console command:

   ```
   START EFTMSERV
   ```

   or

   ```
   S EFTMSERV
   ```

   Where EFTMSERV is the Multiplex Server JCL procedure name provided via the PROCNAME(...) parameter in the installation job.

3. The Multiplex Server log (SYSPRINT and EFTMLOG DD statements) should contain output similar to Figure 1 preceded by date/time information.

4. If the output was produced correctly, the Multiplex Server has started correctly. If not, ensure the Multiplex Server and VTAM configuration parameters were tailored correctly during eFT213 installation.

```
NUAVTAM  NUA2000I NUAVTAM Version 5.5 N24 Compiled DD MMM YYMSERVER
Multiplexed Server started.MSERVER  Trace flag settings: .
MSERVER  Trace flag settings: 0123456789.
EFT     Helper=EXEC 'EFT.N24.LOAD(EFTHELPR)'.
EFT     Service offered.
```

Figure 1. Multiplex Server startup output for eFT213

Stopping the Multiplex Server

1. To stop the Multiplex Server, issue the z/OS console command:

   ```
   STOP EFTMSERV
   ```

   or

   ```
   P EFTMSERV
   ```

   Where EFTMSERV is the name of the Multiplex Server job you submitted or the Multiplex Server started task JCL procedure name. The Multiplex Server should end within about 30 seconds of acknowledging the STOP command.

Update Summary

Version 5.5

651 If LABELNUMBER1 is not specified with LABELTYPE NL or AL, mount will call for SL tape

8012 delete eftutl1 and use __get_cpuid__()

8013 EFT license messages missing at midnight OLDDDNAME only

8017 Reduce bad offer timeout to 1 second

8018 Add 60 second timer for nrb512 stat in offer

8035 Invalid TCP service name 'EFTD' (MUX213-2502).

8072 Update help files for eft

8080 Change getservbyname from dignus code to use IBM resolver code

8107 USE IBM service call gethostbyname

8109 Issue error eft-833 sss service not configured, using program defaults

8139 Add secure transfers to standalone server

8165 Add fipslvl parameter 0-3

8172 Standalone server configuration problem

8175 missing data from show remote

8226 Upgrade to Dignus C 220 and assembler 195 fails in EFT

8230 Missing help modules for build process

8242 Some of the HELP command descriptions have and unusual character

8246 File transfer fails when truncating records

8247 cannot find files to execute

8252 Missing documentation for the configuration keywords in mconf

8253 Local license qualifiers do not follow minimal match rules

8257 Allow configuration of SSL protocol version

8263 OC4 abend when attempting to connect using the NETEX installed version

8266 The 900x license codes are missing in the manual

8267 INSUFFICIENT STORAGE WAS AVAILABLE when accessing EFTLICC at midnight

8278 Upgrade /mnt/zOS/** datasets on unix for dignus compilers ALL dignus complied products

8292 Connections to a service that is not offered are not being retried

8296 Not all debug entries show up when a show debug command is entered

8313 Aliases without HELP entries

8322 Hostnames of all Numbers does not work; should be documented

8352 Keying in HELP shows additional help topics for MVS twice

8451 bad svn rev level for install script

8455 RNT stops after 1st retry attempt fails

8459 missing error messages in the manual

8561 can not log in via standalone server with expiring key

8622 looping send fails after 16000 loops

8696 Local ping command fails with callable service BPX1MSS failed

8714 Segmentation fault when starting the mux server with oldddname specified during the install

Version 5.4.7

477 Add notes about ISPF panels

539 Document PARTialrecord qualifier of send/recv

4783 Add repository info during "build"

5310 Add VCONF/MCONF Parameter Names to Install Parameter Descriptions

6049 APPLID VBUILD <> Member name

6638 Add Password Encrypt alias, clist & job

6814 Remote logon no longer fails with timeout - TSO/E PASSWORDPREPROMPT enabled

7026 Correct FTP instructions in MTU

7837 New ephemeral port range (3100-3999)

7838 Added debug messages at startup

7839 Remote TSO commands displays output

7841 Rename ALOCFILE clist to EFTALOCM

7844 Remove manuals from distribution package

7867 When using -create backup during receive no longer causes an OC4 abend

7869 Remove backup from -CREate send and receive qualifiers

7870 Debug messages no longer coming out on console

7889 Create delete is supported during a receive command

7890 HELPER code supports the DEBUG function

7891 Remote type command now works

Version 5.4.6

- **No Updates**.

Version 5.4.5

- **983, 3346 and 4967:** Added support for static VOLSER symbols.

Version 5.4.4

- **2673:** Can no longer change ROOTDIR while product is running; should be protected.
- **4150:** New license key required to operate from this version forward includes expiration date covering the license term.
- **4776:** Corrected the use of ephemeral port usage causing premature use of a port still in use; symptoms of failure include client unable to connect back to server.
- **4810:** Client now retries connection when server is down.
- **4812:** System ephemeral ports usage is available.

Version 5.4.3

- **3360:** SIO appendage failed to copy during installation due to REPLACE not being specified. The install job was updated to correct this problem.
- **2817:** Intermittent ACF82909 ACF2, WAIT TIME LIMIT EXCEEDED messages and logon failures during remote client logon to eFT213 Server on systems using ACF2.

Version 5.4.2

- **3330:** User abend 3532 may occur when invoking the eFT Client multiple times from within the same TSO session or from within the same TSO batch job step, and SWA=ABOVE is specified for the JES2 JOBCLASS.

Version 5.4.1

- **3236:** S0C4 abend or "Internal Logic Error" message may occur when running the eFT Client either as a batch job or from a TSO user, and SWA=ABOVE is specified for the JES2 JOBCLASS.

Version 5.4

- ISPF Panel Support: Allows TSO/E eFT Clients to use eFT ISPF panels.
- Updated copyright information.
- EFTALLOC, EFTDELOC, and EFTHELPR: New or updated scripts that perform required eFT allocations and deallocations, which makes it easier to implement and use eFT.
- NUALIB: A new DD statement that can be used to point to the eFT load library at Server and/or Client execution.
- TEXTLIB: A new DD statement that is used to point to the eFT ROOTDIR library. This can be used to override the name specified (or defaulted) at installation time.
- RESOLVER Address Space: This is fully supported by this release.
- PORT_MIN and PORT_MAX: These are new configuration parameters that can be used to limit the range of ephemeral ports used by eFT for data connections.
- OLDDDNAMES: This new installation parameter can assist when migrating from USER-Access to eFT by providing support for the SYSERR, SYSPRINT, and SYSIN DD statements.
- Misc bug fixes

Version 5.3.2 N24

- **1375:** Allow all forms of DD (DD: DDN: //DD: //DDN:) to be specified on eFT commands in place of a file name. For example, PUT FILEIN DD:
- **1929:** EFT client SOC4 abend when concatenating DD * to a STDIN.

Version 5.3.1 N24

- **1906:** Server terminates with CC1000 at startup.

Version 5.3.0 N24

This was the initial release of this product. Please refer to "New Features" for additional information.