H304 Secure NetEx/IP®

for Unisys Dorado Systems

Release 1.4

Memo to Users

March 2020

MTU-H304-R1.4

Introduction

This memo provides supplementary and release-dependent information for NetEx users. It should be reviewed carefully prior to installation of the product.

H304, Secure NetEx/IP provides optional secure/private transfers utilizing the same NetEx application interface as legacy NetEx products. Although H304 1.4 is a functionally equivalent product supporting IP communication via CPCOMM without an outboard channel-attached appliance, H304 is NOT compatible or interoperable with all other non-secure NetEx/IP products.

Support

For NetEx/IP and associated products, support is available via:

- 24x7 telephone at (800) 854-0359

- The worldwide web: http://www.netex.com/

- email support@netex.com

Distribution

This product is available via download from our ftp server. This format requires that the release file be transferred to your Unisys system via cpFTP using "bin" and "cfmt" options.

The release is a single program file containing all required executables and utilities.

NetEx Software's policy is to release a distribution for new products without source code.

New Product H304 Release 1.x:

- H304 1.x is functionally equivalent product as H300IPC/H300e. It will co-exist with H300IPC/H300e on the same processor, but is not compatible with other remote H300IPC/H300e or other remote non-secure NetEx/IP products.

- Applications which use Secure NetEx/IP on Unisys platforms will need to be compiled with Extended Mode compilers, and linked with the appropriate application modules. *Basic mode applications are not supported.*

New Product H304 Release 1.4:

Additional hostname resolution features:

- setIP for resolving NetEx hostnames

- restricting inbound connections source IP to the setIP list of IP addresses

- connect timeout parameter

Service Notes

Secure NetEx dumps

Secure NetEx dumps are captured via PADS. The PADS$PF should point to the program file containing the PADS$CONFIG element. Normally this will be in the Secure NetEx configuration library. The USE statement for NTX$DIAG should point to a file that will contain the diagnostic file if the Secure NetEx application abnormally terminates.

CPCOMM PING

In order to test network connectivity, a 'ping' command can be issued from the Unisys host CPCOMM operator interface. The syntax from the "CPCOMM Operator" manual:

[cpcomma] PING HOST,{*host-name | ip-address***} [REPEAT-COUNT,***number***] [BYTES,***number***] ;**
   [WAIT,*seconds***] [RECORD-ROUTE | TIMESTAMP] [LOCAL-IP,***ip-address***]**

.

Update Summary

Release 1.4

8533 Host name resolution additional feature (SetIP)

8583 Add CONNTO for connect timeout

8616 Add feature to restrict the inbound connection to a list of from IP addresses

Release 1.3

8331   Hostnames of all Numbers does not work; should be documented

8393 $ Character Not Valid in Offer IDs - Allow printable characters for hostname and offername

8425   Add realtime support to Secure Netex

8432   Specifying comapi d fails, must be a capital letter

8435   Ability to load custom Character Conversion Tables

8463   SNTX operator interface for termination

8487   Enhance SNX3210I message to include local address and port

Release 1.2

8037 Add multihost support in Secure NetEx

8124 Dump during ntxgenx cleanup after finishing transfer

8133 Add column header to SNXMAPOP 'all'

8147 Move API documentation to another the manual (request from support)

8159 Sync code conversion tables between products

8180 SBFXJS aborts when error "BFX320F BAD CONNECT DATA RECEIVED"

8189 Buffer overflow in data conversion

Release 1.1

7946 SNXMAP does not detect select error

7956 3506 errors are retried instead of failing

7947 Run eat/gen using netex max block

7886 SSL configured for TLSV1 only

7939 BFXTI and BFXTR report different KB transferred when mode is bit

7948 Set NRBSTAT on wait queue NRBs during session cleanup

Release 1.0

This is a new product; therefore there are no updates at this time.