H804 Secure NetEx/IP

for Intel x86 Platforms on Linux Operating Systems

Release 1.5.3

Memo to Users

June 2021

Introduction

This product implements the Network Executive Software Secure NetEx/IP for Intel x86/Linux (H804).

This document should be reviewed carefully prior to installation of H804.

Secure NetEx/IP for Intel x86 for Linux (H804) Release 1.5.3 is NOT compatible or interoperable with other **non-secure** NetEx/IP products on other platforms, as well as with previous releases of H800IP.

H804 is available by download.

The following manual is available for H804:

Hxx4 Secure NetEx/IP Reference Manual(1.5.3)

The manual, along with this Memo to Users can be downloaded from www.netex.com by selecting the 'Support' tab, then navigating to 'Products', then selecting the 'Intel x86/Linux (H80x)' link on the right side of the window, and then clicking on 'Docs' in the 'Secure NetEx/IP [H804]' entry for the appropriate version.

Support

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

* 24x7 telephone at (800) 854-0359

* http://www.netex.com/support

* email: support@netex.com

Notice to the Customer

Comments about this documentation may be submitted via e-mail to support@netex.com or by visiting our website, http://www.netex.com. Always include the complete title of the document with your comments.

Information on Network Executive Software's general software support policy (e.g., alternate contact methods, support severity level descriptions, and service status definitions) may be found at http://www.netex.com/support/software-support-policy.

Software Modification Policy

Modifications to H804 that are not specifically authorized by NESi are prohibited.

Any unauthorized modifications to H804 may affect its operation and/or obstruct NESi's ability to diagnose problems and provide corrections. Any work resulting from unauthorized modifications shall be paid by the customer at NESi's then-current support rates and may result in the immediate termination of warranty/support coverage.

New Features

This product is functionally equivalent to (non-secure) H800IP Release 7.0.4 with the added capability of optionally sending data privately/securely.

Release 1.5.3 Features

- Option to stop connection attempts after a 3501 or 3920 NRBSTAT

Release 1.5 Features

Additional hostname resolution features:

- independent connect from ip address resolution check

Release 1.4 Features

Additional hostname resolution features:

- setIP for resolving NetEx hostnames
- connect timeout parameter
- restricting inbound connections source IP to the setIP list of IP addresses

Release 1.3 Features

Loadable Code Conversion tables.

Release 1.2 Features

Added support for Secure TNP (TNP804) for use with legacy NetEx/IP Requester products.

Multihost support has been added to this release. When enabled, the hostname of the Connect and Offer must match.

FIPS mode has been added to the security settings, as well as specific cipher selection tuning.

Installation

Installation Notes

1. H804 is available as a downloadable distribution. Download instructions can be obtained by contacting support@netex.com.

2. Follow the installation instructions in the appendix for Linux Installation in the Hxx4 *Secure NetEx/IP Reference Manual* to complete the installation.

3. Check if there are any H804 updates by going to www.netex.com, then clicking on the 'Support' tab, then navigating to 'Products', then selecting the 'Intel x86/Linux (H80x)' link on the right side of the window, and then clicking on 'Updates' in the 'Secure NetEx/IP [H804]' entry for the appropriate version. If there are any, download them and follow their installation instructions.

Update Summary

Release 1.0

This is a new product release which is functionally equivalent to the non-secure H800IP Release 7.0.4.

Release 1.2

This is a new maintenance release which has the following tickets addressed:

Ticket	Description
8161	Sync code conversion tables between Hxx4 and H210
8145	Remove API documentation from the manual; available via support@netex.com
8144	Allow tuning of SSL cipher list
8140	NRBSTAT 3202 now in documentation
8135	Add column header to SNXMAPOP 'all'
8117	FIPS mode added to SNXMAP configuration
8115	SNXMAP messages in systemd journal include timestamps
8104	Correct cleanup failure on NetEx Requester transfer.
8103	SNXMAPOP now shows correct license expiration time
8061	SNXMAP now logs to systemd journal
8039	Multihost now supported in Secure NetEx
7965	RFCLEANUP in read processing no longer hangs application
7964	Set NRBSTAT on wait que NRBs during session cleanup
7962	SSL configured for TLSV1 only
7961	Run eat/gen using netex max block
7958	3506 errors are no longer retried
7954	SNXMAP detects select error

Release 1.3

This is a new maintenance release which has the following tickets addressed:

Ticket	Description
8140	NRBSTAT 3202 not in Hxx4 documentation
8144	Allow tuning of SSL cipher list
8161	Sync code conversion tables between Hxx4 and H210
8167	Allow configuration of SSL protocol
8191	Buffer overflow in data conversion
8333	Hostnames of all Numbers does not work; should be documented
8395	$ Character Not Valid in Offer IDs - Allow printable characters for hostname and offername
8489	Enhance SNX3210I message to include local address and port

Ticket	Description
8496	Add serial number to peer certificate message

Release 1.4

This is a new feature release which has the following tickets addressed:

Ticket	Description
8579	Use Unix domain sockets for IPC
8586	Add CONNTO for connect timeout
8599	Host name resolution
8600	Ability to load custom Character Conversion Tables
8618	Add feature to restrict the inbound connection to a list of from IP addresses

Release 1.5

This is a new feature release which has the following tickets addressed:

Ticket	Description
8713	Provide CONIP for allowed connect from IP address

Release 1.5.2

This is a new feature release which has the following tickets addressed:

Ticket	Description
8802	Invalid command 'setconip'
8875	Protect errno from possible change in log message callback
8905	Potential to hang offer port
8909	SNX4217E does not contain correct SSL connect result code
8925	Only export API symbols in shared library
9000	LCLHOST value is not content checked
9003	SOFFR does not validate nrbhost
9007	Hostname value in setip command is not content checked
9038	Resolve snetex service once per session
9053	Move offer conip check from last to first
9057	Consolidate SNXMAPOP output
9082	SNXMAPOP option '-' is ignored
9086	Allow configuration of SNXMAP listen backlog
9092	3506 after seeing 3501
9097	3501 error should have precedence
9098	offers fail with NRB=7

Release 1.5.3

This is a new feature release which has the following tickets addressed:

9141 Add option to stop connection attempts after a 3501 or 3920 NRBSTAT

9145 CNVERIFY does not stop on CN match

9146 Fix status check of OpenSSL functions to load certificates and private keys

9159 SNXMVEAT - Unchecked return value to NULL pointer dereference

9171 Memory leak for secure sessions

9178 SOFFR only accepts one connection