ENTRUST

nShield Security World

nShield Security World v13.4.5 Release Notes

20 March 2024

Table of Contents

1. Introduction

These release notes apply to release of version 13.4.5 of Security World Software for the nShield family of Hardware Security Modules (HSMs). They contain information specific to this release such as new features, defect fixes, and known issues.

The Release Notes may be updated with issues that have become known after this release has been made available. For the latest version, see the Entrust nShield Support portal.

Access to the Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

1.1. Purpose of Security World 13.4.5

Security World version 13.4.5 introduces enhancements as described in this document. It also corrects a number of defects that have been identified in earlier releases.

This release contains updates to the following products:

- Security World Software.
- Updated firmware and Connect images.
- CodeSafe Developer Software.

1.2. Versions of these Release Notes

Revision	Date	Description
3.2	2024-06-11	Terminology change from *firmware image version* to *firmware version*. No content change to the product or the Release Notes.
3.1	2024-03-20	Documentation only update. NSE-53291 has been removed from the list of fixes in Defect fixes in client-side software.
3.0	2023-12-12	Updated to reflect the v13.4.5 release.
2.3	2023-11-21	Republishing from updated documentation tool chain. No content changes to the Release Notes.
2.2	2023-11-03	Update to include warning about nShield 5c image upgrades. See nShield 5c images.

Revision	Date	Description
2.1	2023-09-26	Updated to include details of Audit Logging functionality available in the v13.4 release; see Connect Remote Client Identification in Audit logging. There are no updates to the released versions.
2.0	2023-08-03	Second revision of document, additions for full GA release 13.4.4
1.0	2023-07-20	Initial revision of document

1.3. User documentation

In v13.4, the Security World user documentation was moved from the software package to https://nshielddocs.entrust.com.

- Release notes and user documentation for recent releases are publicly available at https://nshielddocs.entrust.com.
- PDF versions of all supported release notes and user documents are available in the Entrust nShield Help Center at https://nshieldsupport.entrust.com/hc/en-us/categories/360000473317-Documents-Manuals. Access to the Entrust nShield Help Center is available to customers under maintenance. Contact Entrust nShield Technical Support at nshield.support@entrust.com to request an account.

From v13.4, the HSM User Guides are platform neutral. Information for both Linux and Windows operating systems are covered in the same PDF chapters and HTML topics. Differences between the operating systems are called out if and where necessary.

2. Product versions

2.1. Security World software versions

Version	Date	Description
v13.4.3	2023-6-30	First release of 13.4 Security World Software
v13.4.4	2023-7-18	Second release of 13.4 Security World Software
v13.4.5	2023-12-12	Third release of 13.4 Security World Software

2.2. CodeSafe Developer software versions

Version	Date	Description
v13.4.3	2023-6-30	Release of 13.4 CodeSafe 5 Developer software.

2.3. Firmware and nShield Connect ISO versions

Version	Date	Description
v13.4.3	2023-6-30	First release of 13.4 Firmware and Connect ISO, targeted for nShield 5s and nShield 5c only.
v13.4.4	2023-7-18	Second release of 13.4 Firmware and Connect ISO, for all hardware platforms.
v13.4.5	2023-12-12	Third release of 13.4 Firmware and Connect ISO, for all hardware platforms.

2.4. nShield firmware versions

Version	Date	Description
v13.4.3	2023-6-30	First release of 13.4 Firmware for nShield 5s and 5c.
v13.4.4	2023-7-31	Release of 13.4 Firmware for nShield 5s and 5c. Firmware for Solo +, Solo XC, Connect +, and Connect XC are as 13.3 release.
v13.4.5	2023-12-12	Release of 13.4 Firmware for the Solo XC, Connect XC and the nShield 5s and 5c. Firmware for Solo + and Connect + are as 13.3 release.

2.5. nShield Connect image versions

Version	Date	Description
v13.4.3	2023-6-30	First release of nShield Connect images for 13.4 containing the latest features and fixes.
v13.4.5	2023-12-12	Second release of nShield Connect images for 13.4 containing the latest features and fixes.

3. Feature of Security World v13.4.5

3.1. nShield 5s VSN Updates

Impacts: nShield 5s

The 13.4 release contains a VSN increment to a value of 3.

> ❗ This VSN bump impacts the ability to downgrade the nShield 5c image once upgraded to the latest version. See nShield 5c images for more information.

3.2. CodeSafe 5 support added to the nShield 5

Impacts: nShield 5s and 5c

The latest generation of CodeSafe provides improved performance, flexibility, easier and faster network connectivity, additional language support, and developer authentication.

- CodeSafe 5 host application compilation requires GCC compiler version 8.x or later.
- CodeSafe 5 is only compatible with nShield 5s or 5c hardware platforms.
- CodeSafe 5 does not provide host application Java examples, however CodeSafe 5 host application development in Java is still possible.

For usage instructions, see the *CodeSafe 5 Developer Guide* for your HSM.

3.3. Permanently enable ECC on nShield 5s and nShield 5c

Impacts: nShield 5s and 5c

- From 13.4 onwards, the nShield 5s and 5c will report EllipticCurve and AcceleratedECC feature-enable bits permanently "on", and behave as such.

3.4. Concatenation KDF with KMAC is now available

Impacts: clientside software

- KDF algorithm support for 5G development is now available in firmware through the nCore API.

3.5. ARIA support added to the nShield PKCS #11 API

Impacts: clientside software

The following mechanisms are now supported by the nShield PKCS #11 API:

- `CKM_ARIA_KEY_GEN`: this mechanism is used to generate ARIA keys. Supported key lengths: 128, 192 and 256.
- `CKM_ARIA_CBC` and `CKM_ARIA_ECB`: these mechanisms are used when encrypting and decrypting or wrapping and unwrapping with an ARIA key.

Use of these mechanisms requires the `KISAAlgorithms` feature to be enabled, see the *User Guide* for your HSM for more information. See the *nShield PKCS #11 API Reference Guide* for further information on these mechanisms.

3.6. Extended ARIA support in the nShield PKCS #11 API

Impacts: clientside software

The following mechanisms are now supported by the nShield PKCS #11 API:

- `CKM_ARIA_CBC_PAD`: this mechanism is used when encrypting and decrypting or wrapping and unwrapping with an ARIA key.
- `CKM_ARIA_MAC` and `CKM_ARIA_MAC_GENERAL`: these mechanisms are used when signing and verifying with an ARIA key.

Use of these mechanisms requires the `KISAAlgorithms` feature to be enabled, see the *User Guide* for your HSM for more information. See the *nShield PKCS #11 API Reference Guide* for further information on these mechanisms.

3.7. SHA3-based KDF support added to the nShield PKCS #11 API

Impacts: clientside software

The following SHA3-based key derivation functions are now supported by the nShield PKCS #11 API:

- CKD_SHA3_224_KDF, CKD_SHA3_224_KDF_SP800
- CKD_SHA3_256_KDF, CKD_SHA3_256_KDF_SP800
- CKD_SHA3_384_KDF, CKD_SHA3_384_KDF_SP800
- CKD_SHA3_512_KDF, CKD_SHA3_512_KDF_SP800

Use of these key derivation functions requires v13.3 firmware or higher. See the *nShield PKCS #11 API Reference Guide* for further information.

3.8. SHA3-based HMAC support added to the nShield PKCS #11 API

Impacts: clientside software

The following SHA3-based HMAC functions are now supported by the nShield PKCS #11 API:

- CKM_SHA3_224_HMAC, CKM_SHA3_224_HMAC_GENERAL, CKM_SHA3_224_KEY_GEN
- CKM_SHA3_256_HMAC, CKM_SHA3_256_HMAC_GENERAL, CKM_SHA3_256_KEY_GEN
- CKM_SHA3_384_HMAC, CKM_SHA3_384_HMAC_GENERAL, CKM_SHA3_384_KEY_GEN
- CKM_SHA3_512_HMAC, CKM_SHA3_512_HMAC_GENERAL, CKM_SHA3_512_KEY_GEN

Use of these HMAC functions requires v13.3 firmware or higher. See the *nShield PKCS #11 API Reference Guide* for further information.

3.9. Enhanced CKM_RSA_AES_KEY_WRAP support in the nShield PKCS #11 library

Impacts: clientside software

Support for CKM_RSA_AES_KEY_WRAP, in the nShield PKCS #11 library, has been enhanced to reflect updated firmware.

If using CKM_RSA_AES_KEY_WRAP with firmware versions 13.4 or later:

- It is now possible to wrap target keys which have CKA_WRAP_WITH_TRUSTED set.
- It is no longer necessary to override the Security Assurance Mechanisms if the RSA key has CKA_UNWRAP_TEMPLATE set.

If using firmware versions 13.3 or earlier:

- It is not possible to wrap a target key which has CKA_WRAP_WITH_TRUSTED set.
- It will be necessary to override the Security Assurance Mechanisms if the RSA key has CKA_UNWRAP_TEMPLATE set.

See the *nShield PKCS #11 library* section of the *User Guide* for your HSM and the *nShield PKCS #11 API Reference Guide* for further information.

3.10. Relaxed token keys rules

Impacts: clientside software

It is now possible, using C_CopyObject, to change a key's CKA_TOKEN value from CK_FALSE to CK_TRUE. This requires the CKNFAST_JCE_COMPATIBILITY environment variable to be set to 1.

The original key's CKA_TOKEN value will remain unchanged.

See the *User Guide* for your HSM for more information on CKNFAST_JCE_COMPATIBILITY.

3.11. PKCS#11 3GPP performance enhancements

Impacts: clientside software

Performance under loadsharing has been enhanced for TUAK and Milenage signing. It is now possible to control whether session keys will be automatically loadshared or not. Loadsharing adds overhead, but also adds resilience and improves utilization of a multi-module estate. Selection of session keys to be loadshared is by key origin. The default is to loadshare all session keys, which is the previous behaviour.

3.12. HMAC support added to perfcheck and ncperftest

Impacts: clientside software

It is now possible to specify HMAC as the key type for perfcheck and ncperftest when signing or verifying. The following mechansisms are supported:

- HMACSHA256

- `HMACSHA512`
- `HMACSHA3b256`

3.13. Java generic stub and JCE provider support

Impacts: clientside software

The nShield Security World software Java generic stub and JCE provider now supports Amazon Corretto.

3.14. Migration tool options

Impacts: clientside software

The `migrate-world` tool now allows you to select:

- The source OCS or Softcard in the source Security World from which the keys will be migrated.
- A pre-generated OCS or Softcard in the destination Security World into which the keys will be migrated.

3.15. Linux signed RPMs

Impacts: clientside software

The Security World Linux ISO now contains RPM files in the `linux-rpms/amd64` directory. These RPMs should be installable on all supported Linux based operating systems that support RPM packages. See Supported operating systems.

The Codesafe ISO also now contains signed RPMs.

To provide validation of the shipped RPMs, a public key half is shipped on the ISO (under `linux-rpms/amd64`) for verification using the RPM package tooling. Post-install of RPMs should follow the same process as a TAR installation.

3.16. Increased number of connects that can be added to a client

Impacts: clientside software

The number of nShield Connects that can be enrolled to an individual client side software hardserver has been increased to 250.

3.17. Connect Watchdog utility

Impacts: nShield Connect+, nShield Connect CLX, nShield Connect XC, nShield 5c

nShield Connect contains a watch dog facility to provide additional logging information for front panel service operations and failures. This feature is turned off by default, it can be enabled from the front panel. "1-1-12-1 >Enable watchdog"

3.18. Connect Remote Client Identification in Audit logging

Impacts: nShield Connect+, nShield Connect CLX, nShield Connect XC, nShield 5c

Security World Audit Logging functionality has been updated to allow audit logs from the nShield Connect to be traced to the client machine that initiated a command for the HSM.

A new `session` field has been added to audit log messages that contains a unique identifier for the remote client. This identifier is generated when the client initiates the session and a `Cmd_SessionCreate` audit log entry is created to associate the identifier with the client IP address and KNETI hash as in the example below:

```
CEF:0|nCipher Security|nShield Solo|13.4.0|1|Cmd_SessionCreate|1|esn=03A0-D075-
C49A rsid=23 rtc=1557084181642 seqNo=66 source=host outcome=success
description=IP:"192.168.10.21:33044";KNETI:"3952eca167a7dcf251a08b745d53bdfd821a39
3b" session=639b0bc800000001
```

All audit logs for commands issued by that client will then reference the client's unique session identifier (`session=639b0bc800000001` in this case) as in the below example:

```
CEF:0|nCipher Security|nShield Solo|13.4.0|1|Cmd_GenerateLogicalToken|1|esn=03A0-
D075-C49A rsid=23 rtc=1557084181681 seqNo=447 source=host session=639b0bc800000001
outcome=success htok=8512ea2397bb0e407de3ba617b2d5fc33d5a6fe3 sharesneeded=1
sharestotal=1 timelimit=100 hkm=82a0ddfaac7b8a0c8a39afbcbdd4df9a7f3e44dd
```

Termination of that client session (when the Impath resilience session times out or immediately after connection loss if Impath resilience is not enabled in config) is recorded with a `Cmd_SessionDestroy` entry in the log.

The *nShield Connect User Guide* has been updated with full details of the change, see the "Client ID Session Extension" section.

3.19. Connect IPv6 remote syslog support

Impacts: nShield Connect+, nShield Connect CLX, nShield Connect XC, nShield 5c

It is now possible to configure remote syslog using IPv6 addresses. See the *User Guide* for your HSM for more information.

3.20. OpenSSL with NFKM Engine application note

The *OpenSSL with NFKM Engine* application note has been published and is available via https://nshielddocs.entrust.com.

4. Notes for future releases

The following are important notes about up-coming changes in future Security World releases that are being highlighted early.

- The CEF logging subsystem is being replaced with a new Audit Logging system in a future firmware release.
- The Tiger hash algorithm will be removed in a future firmware release.

5. Firmware, nShield Connect images, and certifications

The nShield firmware and nShield Connect image ISO is available which contains all firmware and nShield Connect images supported by this release, the layout of the firmware ISO is that of the 13.3.1 release and includes FIPS certified, Solo+, SoloXC, ConnectXC and Connect+.

This ISO can be obtained through contacting https://nshieldsupport.entrust.com (asking for product code `SW2187C-FW-E`).

5.1. Firmware images

There is no change to the installation of the firmware in 13.4.5.

5.1.1. nShield 5s firmware

Type	Version	Description	Directory	VSN
FIPS Pending	13.2.2	The latest FIPS firmware released as part of the v13.2 release. Firmware is currently FIPS Pending.	`firmware/nShield5s/fips/nShield5s-13-2-2-vsn2.npkg`	2
Latest/Pending	13.4.3	Latest firmware with features from v13.4 release.	`firmware/nShield5s/latest/nShield5s-13-4-3-vsn3.npkg`	3

5.1.2. nShield Solo XC firmware

Type	Version	Description	Directory	VSN
CC Approved	12.60.15	The 12.60 firmware currently certified to the CMTS Common Criteria certification	`firmware/SoloXC/cc/soloxc-12-60-15-vsn37.nff`	37
FIPS Approved	12.72.1	The latest FIPS approved firmware released as part of the v12.72 release.	`firmware/SoloXC/fips/soloxc-12-72-1-vsn37.nff`	37

Type	Version	Description	Directory	VSN
Transition FW	12.50.7	The firmware that can be used for transition from old Solo XC firmware to latest. See nShield Solo XC upgrade notes for more information.	`firmware/SoloXC/transition-fw/soloxc-12-50-7-vsn37.nff`	37
Latest	13.4.3	Latest firmware with features from v13.4 release.	`firmware/SoloXC/latest/soloxc-13-4-3-vsn37.nff`	37

5.1.3. nShield Solo+ firmware

Type	Version	Description	Directory	VSN
CC Approved	2.55.1	The latest CC approved firmware for 11.72. This should be used with Security World 11.72.02 on the client host	`/firmware/Solo/cc/solo-2-55-1-vsn26.nff`	26
FIPS Approved	12.72.0	The latest FIPS approved firmware released as part of the v12.72 release.	`/firmware/Solo/fips/solo-12-72-0-vsn29.nff`	29
Latest	13.3.1	Latest firmware with features and defect fixes from v13.3 release.	`/firmware/Solo/latest/solo-13-3-1-vsn29.nff`	29

The firmware monitor to use with the above nShield Solo+ firmware: `/firmware/Solo/monitor/solo-monitor-2-60-1-vsn26.nff`.

5.1.4. nShield Edge Firmware

There is no updated 13.3 firmware for the nShield Edge. Support for the Edge is still maintained for previous firmware releases.

Type	Version	Description	Directory	VSN
FIPS Approved	12.72.0	The latest FIPS approved firmware released as part of the v12.72 release.	`/firmware/Edge/fips/edge-12-72-0-vsn29.nff`	29

The firmware monitor to use with the above nShield Edge firmware: `/firmware/Edge/monitor/edge-monitor-2-50-16-vsn24.nff`.

5.2. nShield Connect images

The nShield firmware and nShield Connect Image ISO includes v13.4.5 nShield Connect images that contain the Solo+, Solo XC and nShield 5s firmware described in Firmware images.

5.3. Install an nShield Connect image

As part of the Security World installation, the `/opt/nfast/nethsm-firmware` directory is created, but it is empty. When the nShield Connect image that needs to be installed has been chosen, the subdirectory and the image should be copied from the nShield firmware and nShield Connect ISO into the `/opt/nfast/nethsm-firmware` directory and installed onto the nShield Connect as usual.

5.3.1. nShield 5c images

> ❗ Due to the nShield 5s VSN being bumped in the v13.4.3 firmware image, upgrading to the nShield 5c **Latest** image will prevent being able to downgrade to any other released version of nShield 5c image. This includes not being able to downgrade to the 13.4.3 FIPS Pending nShield 5c image.

Type	Version	Description	Firmware included	Directory	VSN
FIPS Pending	13.4.5	13.4 nShield Connect image with FIPS pending firmware	13.2.2	`nethsm-firmware/fips-all-13-4-5-vsn32/nCx3N.nff`	32
Latest	13.4.5	13.4 nShield Connect image with latest 13.4 firmware. See important note above before upgrading.	13.4.3	`nethsm-firmware/latest-all-13-4-5-vsn32/nCx3N.nff`	32

5.3.2. nShield Connect XC images

Type	Version	Description	Firmware included	Directory	VSN
CC Approved	13.3.2	13.3 nShield Connect image with CC approved XC firmware	12.60.15	`nethsm-firmware/cc-xc-13-3-2-vsn32/nCx3N.nff`	32

Type	Version	Description	Firmware included	Directory	VSN
Transition Image	12.50.4	The Connect image that can be used for transition from old Connect XC firmware to latest. See nShield Connect XC image upgrade notes for more information.	3.4.2	`nethsm-firmware/transition-xc-12-50-4-vsn31/nCx3N.nff`	31
FIPS Approved	13.4.5	13.4 nShield Connect image with FIPS approved firmware	12.72.1	`nethsm-firmware/fips-all-13-4-5-vsn32/nCx3N.nff`	32
Latest	13.4.5	13.4 nShield Connect image with latest 13.4 firmware	13.4.3	`nethsm-firmware/latest-all-13-4-5-vsn32/nCx3N.nff`	32

5.3.3. nShield Connect+ images

5.3.3.1. v13.3 and original specification Connect+ compatibility issue

Connect+ images released in v13.3 contain an update regarding Fan controls that are not compatible with original build specification Connect+ units produced from 2012 to 2016. If you have a unit with a serial within the range below, we would advise against updating those to v13:

- `26-NC**`
- `28-NC**`
- `36-NC**`
- `37-NC**`

Please note that there is a VSN increase in the v13 image, so if you do upgrade the device, you will not be able to downgrade to an older image. If you do upgrade, the Fan within the Fan Tray unit will spin at their maximum rated RPM, which will, ultimately, reduce the lifespan of the peripheral part. The Connect+ product range entered End of Life status at the end of 2022.

Type	Version	Description	Firmware included	Directory	VSN
CC Approved	12.45.1	nShield Connect image with CC approved 11.72 firmware	2.55.4	`nethsm-firmware/cc-plus-12-45-1-vsn30/nCx3N.nff`	30

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	13.4.5	13.4 nShield Connect image with FIPS approved firmware	12.72.0	`nethsm-firmware/fips-all-13-4-5-vsn32/nCx3N.nff`	32
Latest	13.4.5	13.4 nShield Connect image with latest 13.3 firmware	13.3.1	`nethsm-firmware/latest-all-13-4-5-vsn32/nCx3N.nff`	32

5.3.4. nShield Connect CLX images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	13.4.5	13.4 nShield Connect image with FIPS approved firmware	12.72.0	`nethsm-firmware/fips-all-13-4-5-vsn32/nCx3N.nff`	32
Latest	13.4.5	13.4 nShield Connect image with latest 13.3 firmware	13.3.1	`nethsm-firmware/latest-all-13-4-5-vsn32/nCx3N.nff`	32

6. Upgrade from previous releases

6.1. Security World Software upgrade

Before installing this release, you must:

- Confirm that you have a current maintenance contract that licenses you to deploy upgrades on each nShield HSM and corresponding client operating system.
- Uninstall previous releases of Security World Software from the client machines.

For instructions, see the *Installation Guide* for your HSM.

6.2. nShield HSM Firmware upgrade

Consult the relevant *Installation Guide* for the particular HSM for instructions on how to upgrade to the required firmware.

6.2.1. nShield Solo XC upgrade notes

The following are important notes to observe when upgrading the Solo XC firmware to the latest version:

6.2.1.1. Transition Firmware

If the Solo XC HSM is installed with the earlier 3.3.10 firmware it cannot be upgraded directly to the latest firmware and needs to be first upgraded to an intermediate version. Please contact nshield.support@entrust.com and request the firmware upgrade patch from 3.3.10 to 3.3.20.

If the nShield Solo XC HSM is installed with firmware earlier than 12.50.7, 12.50.2, 3.4.2 or 3.3.41 it cannot be upgraded directly to the latest firmware and needs to be first upgraded to an intermediate version. Any of the firmware versions listed above can be used as an intermediate version. A suitable transition firmware has been provided on the v13.4.5 Firmware ISO. See nShield Solo XC firmware for details. Please contact nshield.support@entrust.com for any other version of firmware.

6.2.1.2. Solo XC Bootloader update

As part of the v13.3 Solo XC firmware, the Security Processor Bootloader will be upgraded. The first time it is upgraded, it will take slightly longer than subsequent upgrades. The upgrade should take approximately five minutes. During this time the module will reset several times, which can be noted by the module LED steadily pulsing blue intermittently. It is absolutely critical that power remains connected to the host PC throughout the entirety of the upgrade process. If power is removed it is possible for the module to be rendered unusable and unrecoverable.

6.2.1.3. Compatibility

Whilst every effort is made to ensure nShield Solo XC firmware compatibility with all mainstream hardware and virtualized environments as well as operating systems there may be occasions where a particular configuration is not compatible (either through current version or after upgrading to a newer version of the firmware). Please contact nshield.support@entrust.com if you experience any issues following an upgrade or during integration activity.

6.3. nShield Connect image upgrade

As part of the Security World installation, the `/opt/nfast/nethsm-firmware` directory is created, but it is empty. When the nShield Connect image that needs to be installed has been chosen, the subdirectory and the image should be copied from the nShield firmware and nShield Connect ISO into the `/opt/nfast/nethsm-firmware` directory and installed onto the nShield Connect as usual.

Consult the relevant *Installation Guide* for the particular HSM for instructions on how to upgrade to the required image.

6.3.1. nShield Connect XC image upgrade notes

If the nShield Connect XC HSM is installed with image earlier than 12.45, 12.46, 12.50.4, or 12.50.7 it cannot be upgraded directly to the latest nShield Connect image and needs to be first upgraded to an intermediate version. Any of the nShield Connect image versions listed above can be used as an intermediate version. A suitable transition images has been provided on the v13.4.5 Firmware ISO. See nShield Connect XC images for details. Please contact nshield.support@entrust.com for any other version of nShield Connect image.

6.3.2. nShield Connect+ image upgrade notes

nShield Connect+ HSMs running an image earlier than v12 must first be upgraded to a v12 version before being upgraded to v13.3. Please contact nshield.support@entrust.com for further support and access to a relevant transition image.

7. Compatibility

7.1. Supported hardware

This release is targeted at deployments with any combination of the following nShield HSMs:

- nShield 5s (Base, Mid, High)
- nShield Solo XC (Base, Mid, High)
- nShield Solo PCI Express (500+ and 6000+)
- nShield 5c (Base, Mid, High)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield Connect CLX (Base, Mid, High)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Edge
- nToken PCI Express "+" (NC2023E-000)

7.2. Supported operating systems

This release has been tested for compatibility with the following operating systems:

Operating System	Solo+	Solo XC	nShield 5s	Connect+, Connect XC, nShield 5c	Edge
Microsoft Windows 10 x64	Y	Y	Y	Y	Y
Microsoft Windows 11 x64	Y	Y	Y	Y	Y
Microsoft Windows Server 2016 x64	Y	Y	Y	Y	Y
Microsoft Windows Server 2019 x64	Y	Y	Y	Y	Y
Microsoft Windows Server 2022 x64	Y	Y	Y	Y	Y
Microsoft Windows Server 2022 Core x64	Y	Y	Y	Y	**N**
Red Hat Enterprise Linux 7 x64	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8 x64	Y	Y	Y	Y	Y

Operating System	Solo+	Solo XC	nShield 5s	Connect+, Connect XC, nShield 5c	Edge
Red Hat Enterprise Linux 9 x64	Y	Y	Y	Y	Y
SUSE Enterprise Linux 12 x64	Y	Y	Y	Y	Y
SUSE Enterprise Linux 15 x64	**N**	**N**	Y	Y	**N**
Oracle Enterprise Linux 7 x64	Y	Y	Y	Y	Y
Oracle Enterprise Linux 8 x64	Y	Y	Y	Y	Y

Security World v13.4.5 Linux support is restricted to x86/x64 architectures. Additional mainstream x86/x64 based Linux distributions other than those listed above may be compatible, however Entrust cannot guarantee this compatibility.

7.3. API support

7.3.1. Java

The versions in the table below are for both Oracle JDK and Open JDK.

Version	Supported
8	Y
11	Y
17	Y

7.3.2. Python

This lists the versions of Python that are supported.

Version	Supported
2.7	Y
3.10	Y

7.4. Supported virtual environments

Operating System	Solo+	Solo XC	nShield 5s	Connect+, Connect XC, nShield 5c	Edge
Microsoft Hyper-V Server 2016	N	Y	N	Y	N
Microsoft Hyper-V Server 2019	N	Y	N	Y	N
Microsoft Hyper-V Server 2022	N	Y	N	Y	N
VMWare ESXi 7.0	N	Y	N	Y	N
Citrix XenServer 8.2	N	Y	N	Y	N

7.5. Supported compilers for Microsoft Windows C developers

Security World v13.4.5 C libraries for Windows were built using Visual Studio 2017 and have been compiled with the SDL flag. This makes them incompatible with older versions of Visual Studio. This applies primarily to static libraries.

Microsoft Windows developers should upgrade to Visual Studio 2017.

8. Defect fixes

8.1. Defect fixes in client-side software

Reference	Description
NSE-57137	Addressed a memory leak in the CNG provider.
NSE-57123	Missing `debugFuncEnd` added to improve nCipherKM debug output.
NSE-56895	The PKCS#11 library now deletes the template key created if a derive operation fails.
NSE-56698	Fixed an issue with building the nShield 5 drivers on RHEL 8.8.
NSE-56619	Addressed NULL dereference issue that could lead to the hardserver segfaulting during `SessionCreate` with a failed module.
NSE-55554	Fixed an issue with the migrate-world utility not supporting execution through Microsoft PowerShell.
NSE-54706	`nfdiag` now searches for per-user logs in the user home directories and includes extra logs: `raserv.log`, `rfs-sync.log` and `cmdadp-debug.log`.
NSE-53663	Fixed an `nfpython` issue where ACL construction can fail in some cases.
NSE-53525	Updated OpenSSL patches.
NSE-53502	Fixed an issue with `seelib` not allowing commands and replies over 8K.
NSE-52877	When using an nToken in your security world install will not cause remote or virtual slots import to fail.
NSE-52651	When using `CKM_ECDH1_DERIVE`, the PKCS#11 library now accepts `CKK_EC_MONTGOMERY` public key data that is encoded according to RFC 7748.
NSE-50221	The PKCS#11 Security Officer Key (ncipher-pkcs11-so-key) did not have a key generation certificate and did not pass `nfkmverify`. `cksotool` now includes the key generation certificate when generating the Security Officer Key.
NSE-46986	`pubkey-find` utility now recognizes the latest security world Cipher Suites.
NSE-46984	nShield CNG now supports .NET `CngKey.IsEphemeral` property.
NSE-46730	The Java method `destroyMergedKeyID()` would fail with an `ObjectInUse` error. This has been corrected.

Reference	Description
NSE-46399	Under rare circumstances applications could lock up while attempting to retrieve Security World information. This was caused by the hardserver indefinitely repeating a query to an unavailable module, and never returning a reply. This has been corrected.
NSE-43519	12.80 clientside added support for IPv6 in the hardserver, however if IPv6 is disabled on the client machine the hardserver will fail to start. The hardserver will now start if IPv6 is disabled.
NSE-42351	`nfkmverify` now has stricter policy enforcement on keys with unwrap permissions. When a key has `unwrap` permissions, it is better to control the ACLs that may be used to `unwrap` with a key by specifying the hashes of the template key(s) that may be used. `nfkmverify` now produces a warning when it encounters a key that may `unwrap` without any such restriction.
NSE-42104	Fixed an issue with the smartcard insertion timeouts getting reset when the module is cleared.
NSE-41799	An issue has been fixed that could have resulted in error message "unexpectedly returned followup NewEnquiry" being reported in the `hardserver.log`.

8.2. Defect fixes nShield 5s firmware 13.4.3

Reference	Description
NSE-52524	Addressed a memory issue in hardserver `Cmd_GetPublishedObject`.
NSE-51001	Corrected an issue with the reporting of module memory in nShield 5s.
NSE-50120	Fixed an issue related to the minimum battery voltage needed for a bootloader upgrade.
NSE-41609	Fixed an issue with GCM accepting a 0-byte GCM IV.
NSE-41547	Addressed missing FIPS restrictions for `DeriveMech_ConcatenationKDF`.

8.3. Defect fixes in Connect+, Connect CLX, Connect XC, and nShield 5c images

Reference	Description
NSE-57404	Fixed an issue where KNETI can be lost when upgrading to a 13.3 or earlier Connect image from a 12.50 or earlier Connect image which required a factory reset to recover.

Reference	Description
NSE-55122	Fixed an issue related to access control on nShield Connect.
NSE-53282	Fixed an issue where the log file in /opt/nfast/ becomes completely full reaching 16M.
NSE-50232	Adding a client license with `nethsmadmin`, and then through the front panel UI, no longer fails with permission denied.
NSE-48467	Corrected an issue with the nShield Connect front panel UI missing a character from ESN when editing the export slot.
NSE-43482	Connect logs can eventually exhaust all disk space if RFS logging fails or is not configured.
NSE-39264	Fixed an issue where the arrow keys in the front panel UI do not allow you to scroll back.
NSE-22343	Configuring both `[load_seemachine]` and `[dynamics_slots]` on a Connect renders `cfg-pushnethsm` and pulling a config file using the front panel inoperative.
NSE-19460	Pushing a configuration file to a Connect no longer automatically calls `nopclearfail`. The user has to run `nopclearfail` manually.

9. Known issues in Security World 13.4.5

See also Known issues from earlier Security World releases.

Reference	Description
NSE-60554	TUAK and Milenage session key generation performance has decreased due to the need to generate key generation certificates at the point of key generation.
NSE-59415	Unable to load the 13.4.5-fips Connect image on an nShield 5c when 13.4.5-latest already loaded.
NSE-56418	`csadmin ids add` mentions to enable "SEE Activation (Restricted)" when it should be "SEE Activation CodeSafe 5".
NSE-55780	Starting a CodeSafe 5 SEE machine on an nShield 5c mentions "Could not find nshield network interfaces for service discovery" in the verbose output.
NSE-55436	When specifying a destination card set you cannot select by card set hash if the Label of the card set is identical and the migration will produce an error with "Destination world has indistinguishable Cards".
NSE-55428	Building classic Codesafe examples fails with older compiler.
NSE-55378	Minor inconsistency when enabling autostart via `csadmin config`.
NSE-55341	Non human readable error when a random certificate is attempted to be added via `csadmin ids add`.
NSE-55142	From 13.4 keys generated using ckrsagen will now produce a warning using `nfkmverify`, this is due to stricter policy enforce on `unwrap` permissions. To overcome this use `CKA_UNWRAP_TEMPLATE` when generating PKCS#11 keys.
NSE-54569	When `NFAST_KEYPROT_PASS` is in place `hsmdiagnose` asks for Updater password twice.

10. Known issues from earlier Security World releases

These issues are still present in 13.4.5.

Reference	Description
NSE-48073	nShield Connect+ models running software earlier than v12 must first be upgraded to a v12 version before being upgraded to v13. See section *Upgrade from previous releases* for more details.
NSE-46612	There is an issue that can lead to an nShield 5s card to not be recognized on the PCIe bus on server cold boot and the card will show a 2-2-2 BIOS code. This will be addressed in a subsequent release. This only affects cold boot, so the workaround is to reboot the server after start up if the device is not detected.
NSE-54352	There is a known issue with the updated RTC functionality in the nShield 5s that causes it to drift more than expected. It is recommended that if the RTC of the HSM is required, that the RTC is updated with the `--adjust` option every 12 hours to ensure it is able to keep time.
NSE-54512	On the nShield 5s, when checking the firewall status via `systemctl`, the logs can show: + ERROR: INVALID_ZONE: nshield This can be ignored and does not impact the operation of the HSM.
NSE-39031	In Security World v12.10 a compliance mode was added to the nShield Connect to allow compliance with USGv6 or IPv6 Ready requirements.
NSE-28462	During key migration, if an incorrect OCS passphrase is entered, the tool will output the message: Error: Cannot migrate security world. Failed to load softcard <card_name> : wrong passphrase The 'Error: Cannot migrate security world' message is erroneous and can be ignored. The tool will continue and reprompt for the correct passphrase. Once the correct passphrase is entered the key migration will continue and complete successfully.
NSE-28606	Entrust do not recommend migrating keys to non-recoverable worlds since it would then be impossible to migrate the keys in future should the need arise. If keys are migrated into a non-recoverable world then it is not possible to verify OCS and softcard protected keys directly with `nfkmverify`. The OCS or softcards must be preloaded prior to attempting to verify the keys.

Reference	Description
NSE-24335	This issue applies to 12.50.11 XC firmware only. As a result of work to improve the upgrade experience with Solo XC it is necessary to add the following lines to `/etc/vmware/passthru.map` for successful operation of Solo XC in an ESXi environment. # Solo XC 1957 082c link false
NSE-23982	While resetting password if user enters incorrect password, cli prompt prints lone "I". This is where login handler program would print "Incorrect password for cli" message. Only "I" gets through the wire in time due to slow baud rate of the connection. This error is trivial and is only seen at the first log in during password reset.
NSE-23412	Customers should download at minimum CMAKE 3.9 for their RHEL distribution to be able to build the shipped examples.
NSE-25401	When installing 12.60 on a Dell XPS 8930 PC, a "Files in Use" screen may be displayed where it prompts to close down and restart Dell, Intel and NVIDIA applications. This can be ignored.
NSE-25626	Cancelling a Windows installation of the nShield Software with the "nShield Trusted Verification Device" component selected may leave the CyberJack Base Components installed on the machine. The user must restart their machine and uninstall the CyberJack Base Components manually via Add/Remove programs to completely uninstall.
NSE-22337	Users installing on a Pre-Windows 10 machine should download the Windows KB2999226 update to ensure the nShield Software will install correctly.
NSE-26559	If there are symbolic links within the `NFAST_KMDATA` folder then the installation will pause. To rectify the issue remove any symbolic links that may exist within `NFAST_KMDATA` and re-run the installer.
NSE-14406	In the Connect config file the `remote_sys_log` config entry implies multiple entries can be defined but only one remote syslog server can be configured.
NSE-14978	If `Cmd_ChannelOpen` is called without a key id an audit log message will be generated. This can occur if, for example, if `Cmd_Hash` is being used to hash a large amount of data. The nShield code translates this to opening a channel in Sign mode without a key. This would normally not be logged unless the key had the `logkeyusage` permission group flag. However, without a key the necessary checks cannot be performed and the `Cmd_ChannelOpen` is logged. This can be identified as a log entry without a key hash.

Reference	Description
NSE-14519	The enquiry utility in 12.0 client-side incorrectly reports 12.50/12.60 Connect modules as Failed. This is a reporting error in this utility only and does not affect other applications. To confirm the module is in fact usable it is possible to send a `NoOp` command with: nopclearfail -n -m 1
NSE-14362	Type 0 smart cards cannot be used in a FIPS level 3 enforced Security World (introduced in Security World v12.50). Contact Support if you need information on moving from type 0 smart cards to supported smart cards.
NSE-15762	Some instability has been seen in the CNG nShield Service Agent when HSMs report failure after being cleared.
NSE-15834	After disabling key recovery in a Security World (using `killrecov`), `nfkmverify` no longer verifies the Security World, reporting "ACL of NSO not of expected form". The Security World is still usable and key recovery has been disabled.

11. Documentation updates

For this release, the *nShield nToken Install Guide* has been removed because Entrust no longer supplies or maintains the nToken. The installation guide is still present in the documentation for previous Security World versions.