nShield Security World

# nShield Security World v13.2.4 Release Notes

11 October 2024

# Table of Contents

# 1. Introduction

These release notes apply to the release of version 13.2.4 of Security World Software for the nShield family of Hardware Security Modules (HSMs).

These release notes contain information specific to this release such as new features, defect fixes, and known issues. They may be updated with issues that have become known after this release has been made available. For the latest version, see https://nshieldsupport.entrust.com/hc/en-us/sections/360001115837-Release-Notes Access to the Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

We continuously improve the user documents and update them after the general availability (GA) release. Changes in the document set are recorded in these release notes and are published at https://nshielddocs.entrust.com.

## 1.1. Updated nShield Software Release Policy

Entrust has recently introduced an update to the nShield Software release policy to better define the type of release and the associated update and support policy. As part of this, the concept of Long Term Support (LTS) and Standard Term Support (STS) software releases has been introduced, with each software release being either a LTS or STS release.

For more information on the software release policy, see the nShield Security World Release Information. Alternatively contact https://nshieldsupport.entrust.com for more information.

# 2. Purpose of Security World v13.2

Security World version v13.2 is a Standard Term Support (STS) release with the nShield 5s firmware released as a Long Term Support Certified (LTS-C) Firmware following the firmware getting FIPS 140-3 Level 3 certified. This means the 13.2.4 nShield 5s firmware is a LTS-C firmware and supported for an extended period.

This release introduced support for the nShield 5 HSM products (nShield 5s and nShield 5c). This release does not contain any updates for the Solo+, Solo XC, Connect+, Connect XC or Edge products.

The Security World Clientside software and the nShield 5c released as v13.2 was a Standard Term Support (STS) release and is now no longer supported. The 13.2.4 LTS-C 5s firmware should be used with the current LTS Security World release (the v13.6 release). See nShield Software Support Details for details of the latest release, release notes and support dates of this firmware. These release notes have been updated to include information required for the nShield 5s LTS-C firmware only.

An newer version of nShield 5s firmware is now available as a FIPS 140-3 Level 3 certified release. This firmware, v13.4, contains a number of additional fixes and improvements (including CodeSafe 5 support) and is the recommended firmware for use in a nShield 5s FIPS configuration. Contact https://nshieldsupport.entrust.com for more information on and access to this later firmware.

## 2.1. FIPS Approved Firmware release

nShield HSM firmware v13.2 has been certified to FIPS 140-3 Level 3. The following table lists the full details of the v13.2 FIPS approved firmware versions and links to the security policy and FIPS certificate.

| HSM | Certified Release | Version Info | FIPS Level | Certificate | Security Policy |
|---|---|---|---|---|---|
| nShield 5s | v13.2 | • primary-version: 13.2.4<br>• recovery-version: 13.2.4<br>• uboot-version: 1.1.0 | 140-3 Level 3 | 4745 | Security Policy |

## 2.2. nShield 5 Adoption Guide

A new nShield 5 Adoption Guide has been created which contains detailed information on how to adopt the nShield 5 HSM into an existing Security World of nShield XC HSMs. Consult this guide, as well as the v13.2 product documentation, for information about adopting the new nShield 5 HSM.

## 2.3. Versions of these Release Notes

| Revision | Date | Description |
|---|---|---|
| 1.3 | 2024-10-11 | Update to include information about the new 13.2.4 nShield 5s Firmware following FIPS 140-3 Level 3 certification. |
| 1.2 | 2024-06-11 | Terminology change from *firmware image version* to *firmware version*. No content change to the product or the Release Notes. |
| 1.1 | 2024-01-24 | PDF branding update. No content change to the product or the Release Notes. |
| 1.0 | 2022-05-20 | Initial revision of document for release with v13.2.2 |

# 3. Product versions

## 3.1. nShield firmware versions

| Version | Date | Description |
|---|---|---|
| v13.2.4 | 2024-06-28 | Updated release of v13.2 firmware for the nShield 5s HSM. This firmware is FIPS 140-3 Level 3 certified. |
| v13.2.2 | 2022-05-20 | First release of v13.2 Firmware for the nShield 5s HSM. This firmware is FIPS Pending. |

# 4. Updates in nShield 5s 13.2.4

The original v13.2 release included a v13.2.2 version of nShield 5s firmware that was submitted for FIPS 140-3 Level 3 certification. This firmware was updated to v13.2.4 and the resultant v13.2.4 firmware is FIPS certified. Customers using v13.2.2 nShield 5s firmware who require FIPS certification should upgrade to v13.2.4.

The changes made to the firmware were for FIPS certification reasons and have no functional impact on the release.

## 4.1. 13.2.4 upgrade and Recovery image

The 13.2.4 includes both an updated primary and recovery image for the nShield 5s. See Upgrade nShield 5s HSM Firmware for details on how to upgrade the nShield 5 firmware and details of the versions to ensure the HSM is in a valid FIPS configuration.

13.2.4 contains an update to the nShield 5 VSN. Once the firmware is upgraded to 13.2.4 the HSM will not be able to downgrade to the previous v13.2.2 release.

# 5. Features of Security World v13.2

## 5.1. nShield 5s and nShield 5c Hardware

Security World v13.2 introduces support for the new nShield 5 HSM hardware (nShield 5s and nShield 5c).

### 5.1.1. nShield 5s

The nShield 5s is a new HSM with a PCIe form factor. The hardware is similar to that of the nShield Solo XC with the following main differences:

- Fanless operation
- Mode change switch has been removed
- DIP switches for disabling remote operation have been removed
- "Clear" button repurposed as "Recovery" button
- Updated internal components including update to 8 GB RAM
- Status LED is now a tri-color LED

### 5.1.2. nShield 5c

The nShield 5c is a new network attached form factor HSM.

Externally the nShield 5c will look very similar to the Connect XC, however internally the 5c has received a number of upgrades, namely:

- Updated processor (Intel i5)
- Updated fans
- New airflow ducting to support the nShield 5s
- Internal module is an nShield 5s

The nShield 5c comes with serial console as default.

## 5.2. nShield 5 features

Both the nShield 5s and nShield 5c introduce the following features:

### 5.2.1. Performance improvements

The nShield 5 includes improved crypto performance.

The nShield 5 is released in three different speed variants: Base, Mid and High. These offer different levels of cryptographic performance. It is possible to upgrade the speed variant of an nShield 5 HSM that has already been commissioned by purchasing feature certificates.

### 5.2.2. New Firmware Architecture

The architecture of the nShield 5 firmware has been updated to be service oriented and container-based. This will allow for multi-layer security and a clear separation of roles, to support a future multi-tenant environment. No hardware upgrades or changes will be required to enable multi-tenant features when they become available.

A new set of tools accessed via the `hsmadmin` command is provided to manage the user aspects of the new architecture.

### 5.2.3. Communications

The communication protocol between the nShield 5s and the host has been updated to be based on the standard SSH protocol.

It is important that the SSH keys used for communication are managed properly. If the keys are lost or deleted it will not be possible to communicate with the HSM without first performing a recovery procedure. Follow the procedures in the *Installation Guide* and *User Guide* carefully when performing upgrades or changes to installations.

## 5.3. nShield 5 v13.2 limitations

The v13.2 nShield 5s firmware has the following limitations. These have been addressed in later versions of nShield 5s firmware and Security World Software.

- No virtual environment support on the nShield 5s (nShield 5c supports the virtual environments); see Supported virtual environments for details.
- No CodeSafe support - A firmware upgrade will be required to support CodeSafe.
- No option pack support - none of the current option packs support this release of v13.2 Security World Software

# 6. Firmware and certifications

Firmware is available on the nShield firmware and nShield Connect image ISO that is available as download only. The latest LTS release (Security World v13.6) contains the v13.2 FIPS approved nShield 5s firmware detailed below. This ISO can be obtained through contacting https://nshieldsupport.entrust.com (asking for product code `SW2187C-FW` on the v13.6 release).

nShield 5c image that contains this v13.2.4 HSM firmware is available as part of the Security World v13.6 LTS release.

## 6.1. Firmware images

### 6.1.1. nShield 5s firmware

Firmware for the nShield 5s is provided in a new format referred to as an `npkg` and is loaded with the `hsmadmin upgrade` command. For more information on loading the firmware please consult the new *5s User Guide*.

| Type | Version | Description | Directory | VSN |
|---|---|---|---|---|
| **FIPS Approved** | 13.2.4 | FIPS Approved firmware | `firmware/nShield5s/fips/nShield5s-13-2-4-vsn4.npkg` | 4 |

### 6.1.2. nShield 5s Recovery image

| Type | Version | Description | Directory |
|---|---|---|---|
| **FIPS Approved** | 13.2.4 | FIPS approved nShield5s Recovery image. | `firmware/nShield5s/latest/nShield5s-recovery-13-2-4.npkg` |

# 7. Upgrade from previous releases

## 7.1. Install Security World Software

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.
- Install the latest LTS release of Security World Software.

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

The instructions in the *Installation Guide* assume that the HSM being installed has not previously been installed and is in 'factory state' which means that it is using the factory default SSH key. If the HSM being installed has been installed previously it may contain non-default SSH keys. See the instructions in the *User Guide* for how to install HSMs in this state.

## 7.2. Upgrade nShield 5s HSM Firmware

As detailed in the *nShield HSM User Guide*, the nShield 5s HSM firmware consists of 3 major components:

- Primary Image
- Recovery Image
- Bootloader

During normal operation, the nShield 5s is running firmware that is loaded from the Primary image. If required, the nShield ts can be forced into recovery mode to run firmware loaded from the Recovery image. The main purpose of recovery mode is to allow essential maintenance activities that are not possible in when the nShield 5s is running the primary image firmware.

This release supplies updated versions of the primary and recovery HSM firmware and all need to be upgraded to be in a valid FIPS approved configuration. Details for upgrading the different components are detailed in the following section.

### 7.2.1. nShield 5s Firmware Version Check

Following the upgrade, the nShield 5s the primary image, recovery image and bootloader versions can be checked using the hsmadmin command:

```
hsmadmin status --json
```

Following the upgrade, it should report as follows:

```
"mode": "primary",
"primary-version": "13.2.4-280-7f4f0c24",
"recovery-version": "13.2.4-280-7f4f0c24",
"uboot-version": "1.1.0-1245-b9bedfa",
```

If this is reported, the nShield 5s is in a valid FIPS 140-3 Level 3 certified configuration.

### 7.2.2. Upgrading the nShield 5s Primary & Recovery Image

Upgrade packages may contain updates for any of these components. The same upgrade method is used in all cases. The system will automatically detect which components are included in the update package and will load the firmware to the correct location.

It is not recommended to upgrade both the Primary and Recovery images at the same time. The recommended procedure is to upgrade the Primary firmware first. Test that the system performs as expected and then upgrade the Recovery firmware at a later date.

The primary and recovery images can be upgraded using the following command:

For primary:

```
hsmadmin upgrade nShield5s-13-2-4-vsn4.npkg --esn module-esn
```

and for recovery:

```
hsmadmin upgrade nshield5s-recovery-13-2-4.npkg --esn module-esn
```

# 8. Compatibility

## 8.1. Supported hardware

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

- nShield 5s (Base, Mid, High)

## 8.2. Supported operating systems

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

| Operating System | nShield 5s |
|---|---|
| Microsoft Windows Server 2022 x64 | Y |
| Microsoft Windows Server 2019 x64 | Y |
| Microsoft Windows Server 2019 Core x64 | Y |
| Microsoft Windows Server 2016 x64 | Y |
| Microsoft Windows 10 x64 | Y |
| Red Hat Enterprise Linux AS/ES 7 x64 | Y |
| Red Hat Enterprise Linux AS/ES 8 x64 | Y |
| SUSE Enterprise Linux 12 x64 | Y |
| SUSE Enterprise Linux 15 x64 | Y |
| Oracle Enterprise Linux 7 x64 | Y |
| Oracle Enterprise Linux 8 x64 | Y |

Security World v13.2.4 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.

## 8.3. Supported virtual environments

| Operating System | nShield 5s |
|---|---|
| Microsoft Hyper-V Server 2016 | N |

| Operating System | nShield 5s |
|---|---|
| Microsoft Hyper-V Server 2019 | N |
| VMWare ESXi 6.7 | N |
| Citrix XenServer 8.2 | N |

# 9. Known and fixed issues

The table below lists known and fixed issues in the 13.2.4 firmware. For details of known and fixed issues in the nShield 5c or clientside used with this firmware, consult the relevant Security World release notes for that release.

| Reference | Scope | Status | Description |
|---|---|---|---|
| NSE-42034 | Firmware | Resolved | Cmd_Encrypt does not properly populate the returned M_IV structured for Mech_AESmGCM. If an IV was supplied to Cmd_Encrypt then this value can be used instead. If no IV was supplied to Cmd_Encrypt then, for Mech_AESmGCM, the default chosen has taglen=16 and aad=the empty byteblock. |
| NSE-40180 | Firmware | Resolved | Integrity mechanisms can be used with DeriveMech_RawDecrypt. |
| NSE-41351 | Firmware | Resolved | During module initialization, module state certificates use KLF2 in all security world types. Formerly, legacy world types used the now-deprecated KLF. |
| NSE-41139 | Firmware | Resolved | Validation of elliptic curve cryptography domains was tightened to reject additional pathological cases. |
| NSE-37311 | Firmware | Resolved | The minimum embedding degree of custom elliptic curve domains was increased to 100, in line with FIPS requirements. |
| NSE-34754 | Firmware | Resolved | Policy checking on elliptic curve cryptography domains was made more independent of representation. |
| NSE-33382 | Firmware | Resolved | DeriveMech_HyperledgerClient was extended to support KeyType_ECPrivate, in line with other ECC mechanisms. |
| NSE-40186 | Firmware | Resolved | API documentation for DSAComm, DSACommVariableSeed and DSACommFIPS186_3 was improved. |
| NSE-41497 | Firmware | Resolved | API documentation for DeriveMech_AESKeyWrap, DeriveMech_AESKeyUnwrap and Mech_AESKeyWrapPadded were improved. |
| NSE-39505 | Firmware | Resolved | API documentation for the SupportsAuthentication flag was corrected. |
| NSE-35407 | Firmware | Resolved | API documentation for ECDSA and KCDSA signature mechanisms was improved. |
| NSE-28534 | Firmware | Resolved | Multiple NIST and other specification references were added to nCore API documentation. |
| NSE-47044 | Firmware | Open | The reset of the nShield 5s that occurs when using hsmadmin reset, factorystate or upgrade may not work reliably in some servers. A restart of the server may be required. |

| Reference | Scope | Status | Description |
|---|---|---|---|
| NSE-46925 | Firmware | Open | If the hsmadmin keys backup command is used to write to a folder rather than an individual file it will set permissions of the folder to which the key is written. This may cause problems if the folder already existed and had different permissions. It is recommended that the backup key is always written to a folder specifically created for the purpose. |
| NSE-46123 | Firmware | Open | The ECDHKA, X25519KA, ECIESKeyWrap and ECIESKeyUnwrap key derivation mechanisms are not available in the 13.2 released firmware, and will return an UnknownMechanism status. The corresponding PKCS#11 mechanisms will also be unavailable. |
| NSE-42504 | Firmware | Open | If the hsmadmin reset command is used without first putting the nShield 5s into maintenance mode, the module will be marked as failed in enquiry until ""nopclearfail -r"" is run, or the hardserver is restarted. |
| NSE-40144 | Firmware | Open | If the nShield 5s device driver is installed in a Windows server before the hardware is installed, an additional reboot will be required before the card will be recognized. |