nShield Security World

nShield Security World v13.3 Release Notes

18 October 2024

Table of Contents

1. Introduction

These release notes apply to release of version 13.3 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 v13.3

Security World v13.3 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
- Firmware for all supported HSMs
- nShield Connect images for all supported HSMs
- CodeSafe Developer Software
- Remote Admin Client

Please read the following release notes, in particular the Upgrade from previous releases section for important notes on upgrading to the latest release.

1.2. Versions of these Release Notes

Revision	Date	Description
1.3	2024-06-11	Terminology change from *firmware image version* to *firmware version*. No content change to the product or the Release Notes.
1.2	2024-04-05	URL syntax fix for the HTML version. No content changes.
1.1	2023-07-27	Addition of note around v13.3 not being supported on the original build specification of Connect+ models. See v13.3 and original specification Connect+ compatibility issue for details.
1.0	2023-03-31	Initial revision of document for the release of Security World v13.3

2. Product versions

2.1. Security World software versions

Version	Date	Description
v13.3.2	2023-3-31	First release of 13.3 Security World Software

2.2. CodeSafe Developer software versions

Version	Date	Description
v13.3.2	2023-3-31	First release of 13.3 CodeSafe Developer software

2.3. Firmware and nShield Connect ISO versions

Version	Date	Description
v13.3.2	2023-3-31	First release of 13.30 Firmware and Connect ISO, including the release of firmware (13.3) and nShield Connect image (13.3) along with FIPS and CC approved firmware and Connect images.

2.4. nShield firmware versions

Version	Date	Description
v13.3.1	2023-3-31	First release of 13.3 Firmware for all HSMs containing the latest features and fixes.

2.5. nShield Connect image versions

Version	Date	Description
v13.3.2	2023-3-31	First release of nShield Connect images for 13.3 containing the latest features and fixes.

3. New features of Security World v13.3

3.1. nShield 5 General Updates

See nShield 5s and nShield 5c hardware for details of the new nShield 5s and nShield 5c hardware.

3.1.1. nShield 5s VSN Improvements

Impacts: nShield 5s

Every nShield 5s records the minimum firmware VSN that it will accept. This is now set manually as opposed to using the VSN of the firmware installed. To increase the HSM's minimum VSN requirement, the `hsmadmin setminvsn` command is used. The new VSN must be greater than or equal to the HSM's current minimum required VSN, and cannot be greater than the VSN of the firmware currently installed on the HSM.

The firmware can be upgraded to a new firmware version with an equal or higher VSN than the minimum VSN set on module, even if the firmware currently installed on the module has a higher VSN than the firmware to which you are upgrading. You can never load firmware with a lower VSN than the target HSM's minimum VSN requirement.

For example, if the HSM has a minimum VSN requirement of 3 and the currently installed firmware has a VSN of 4, you can install firmware with a VSN of 3 or above to the HSM. You cannot install firmware with a VSN of 1 or 2 to this HSM.

Therefore it is possible to upgrade to a firmware version with a higher VSN that the HSM's current firmware without committing yourself to the upgrade. The older firmware can be reinstalled at any time provided the `hsmadmin setminvsn` command has not set the minimum VSN to a higher value.

The VSN is used to prevent future downgrades of the firmware that could potentially weaken security. It is therefore recommended that the `hsmadmin setminvsn` command always be used as soon as the decision has been made not to return to the older version of the firmware.

More details, including the requirements on setting the minimum VSN, is detailed in the *5s User Guide*.

The nShield 5c shares the same VSN functionality as the other Connect products (i.e. Connect+ and Connect XC) and so these improvements do not apply to the nShield 5c.

3.1.2. New Security protections for client keys

Impacts: nShield 5s, nShield 5c

Security World v13.3 adds new security protections for client keys for nShield 5 modules. Existing nShield 5 client keys created with v13.2 software will continue to work, but if the new protections are wanted in existing nShield 5 deployments, the keys can be regenerated with the `hsmadmin keys roll` command. It is recommended that the `sshadmin` key be backed up using `hsmadmin keys backup --passphrase` if the HSM may be moved to a new host machine in future. See the *User Guide* for more information on client key protection options.

3.1.3. nShield 5s Environmental Monitoring

Impacts: nShield 5s

A new command has been added to the nShield 5s, `hsmadmin getenvstats`, that provides the environmental monitoring statistics of the HSM. Environmental monitoring statistics available depend the version of the firmware installed on the HSM.

3.1.4. nShield 5s RTC

Impacts: nShield 5s and nShield 5c

Improvements have been made to the Real Time Clock (RTC) on the nShield 5s.

The method of setting and getting the RTC on the nShield 5s has also changed. Previously the RTC on the nShield 5s was set using the nCore command `Cmd_SetRTC` and retrieved using the nCore command `Cmd_GetRTC`, however for the nShield 5s on v13.3 firmware, this functionality has been moved to the `hsmadmin` command utility.

New commands have been added to the `hsmadmin` command:

- `settime` - sets the system date and time of the HSM. The nShield 5s will need to restart following this command being run.
- `settime --adjust` - smoothly adjusts the system time of the HSM to the new time value.
- `gettime` - returns the system date and time of the HSM.

Consult the *nShield 5s user guide* for more details of these new commands.

3.1.4.1. Setting RTC Authorization changes

Setting the RTC on the nShield 5s no longer requires ACS authorization, however there are restrictions on setting the RTC time, specifically:

- RTC cannot be set to a date or time earlier than the build date of the current firmware.
- Once initially set, the RTC cannot be set to an earlier date or time. The HSM needs to be factory stated (which will remove it from the current Security World) before the HSM will allow the RTC to be set to an earlier date or time.

3.1.4.2. nShield 5c

Setting and getting the RTC on the nShield 5s within the nShield 5c can be done via:

- Serial CLI interface, which is done using the new `setrtc` and `getrtc` commands.
- Front panel

Note: There is currently no mechanism to adjust the RTC of the 5s in the 5c once the time has been set. This will be addressed in a future release.

The nShield 5c will need to reboot following the setting of the RTC.

3.1.5. nShield 5c log retrieval

Impacts: nShield 5c

The nShield 5s introduced a `hsmadmin logs` command that allows the retrieval of logs from the nShield 5s HSM. These logs where not able to be obtained from the nShield 5s inside a nShield 5c. In Security World v13.3 a new Serial Console command, `logs` has been added that will print out the logs from the nShield 5s.

3.2. Solo XC General Updates

Impacts: nShield Solo XC, nShield Connect XC

See Upgrade from previous releases for important notes about upgrading to the latest Solo XC firmware and Connect image.

3.2.1. Solo XC RTC

Improvements have been made to the Solo XC Real Time Clock (RTC) to prevent loss of time during HSM or hardserver restarts.

3.2.2. Solo XC SEE size

In CodeSafe versions prior to 13.3, the Solo XC only supported SEE machines smaller than 70 MB. From 13.3 onwards, the Solo XC supports SEE machines of up to 800 MB.

3.3. HSM User Flash stats

Impacts: nShield Solo XC, nShield 5s

Additional reporting has been added to stattree to report on the NVRAM in the HSM with the following new stats:

- `nvmFreeSpace` - Free space available on the HSMs NVRAM, in bytes
- `nvmWearLevel` - Wear level of the HSM's NVRAM
- `nvmWornBlocks` - Worn blocks in the HSM's NVRAM

3.4. Additional SHA-3 support in firmware and nCore API

Impacts: nShield Solo+, nShield Solo XC, nShield 5s

Additional support for SHA-3 has been added to the v13.3 firmware and nCore API in the fol lowing:

ECDSA Mechanisms

- `ECDSAhSHA3b224`
- `ECDSAhSHA3b256`
- `ECDSAhSHA3b384`
- `ECDSAhSHA3b512`

RSA PKCS#1 Signature Mechanisms

- `RSAhSHA3b224pPKCS1`
- `RSAhSHA3b256pPKCS1`
- `RSAhSHA3b384pPKCS1`
- `RSAhSHA3b512pPKCS1`

HMAC Key Types and Mechanisms

The following key types and mechanisms have been added for HMAC SHA-3:

- `HMACSHA3b224`

- HMACSHA3b256
- HMACSHA3b384
- HMACSHA3b512

SHA-3 for KDFs

SHA-3 supported has been added to the following DeriveMech KDF mechanisms, with support added for SHA3b224Hash, SHA3b256Hash, SHA3b384Hash and SHA3b512Hash:

- DeriveMech_ConcatenationKDF
- DeriveMech_ECCMQV
- DeriveMech_ECCMQVdNISTCKDF
- KAParams.kdfhash

3.5. HMAC as a KDF

Impacts: nShield Solo+, nShield Solo XC, nShield 5s

Support has been added to the v13.3 firmware and nCore API to support HMAC as a KDF. A new DeriveMech_RawSign mechanism has been added to support this.

This is mechanism is not permitted in FIPS Level 3 Security Worlds.

3.6. KMAC

Impacts: nShield Solo+, nShield Solo XC, nShield 5s

Support has been added to the v13.3 firmware and nCore API to support KMAC, specifically:

- KMAC128
- KMAC256

These have been implemented in line with SP800-185 and are permitted in all Security World modes.

3.7. 3GPP/5G Algorithm Support

Impacts: nShield Solo+, nShield Solo XC, nShield 5s, clientside software

Security World v13.3 has added native and PKCS#11 support for 3GPP/5G subscriber

authentication features MILENAGE, TUAK and SIDF.

3.8. User-supplied IVs for key wrapping with GCM

Impacts: nShield Solo+, nShield Solo XC, nShield 5s

In Security World firmware v12.60, v12.70 and later, a change was made that prohibits the use of `Mech_RijndaelmGCM` with the following mechanisms:

- `DeriveMech_RawEncrypt`
- `DeriveMech_RawEncryptZeroPad`
- `DeriveMech_PKCS8Encrypt`

This was done due to a vulnerability that showed that using the AES-GCM mechanism for wrapping key material was insecure, if an attacker could encrypt known key data using the same IV. The recommended solution to this problem was to require each AES-GCM encryption to use a fresh IV value, randomly chosen by a trusted source (e.g. an HSM).

A new mechanism `Mech_AESmGCM` was provided that was permitted with the `DeriveKey` mechanisms, but does not accept a user-supplied IV. Instead, each encryption uses a fresh IV, generated randomly by the HSM.

Security World v13.3 now adds a method of allowing key wrapping using AES-GCM and a user-supplied IV. To do this, without compromising the security of existing keys, three new `DeriveKey` mechanisms have been introduced:

- `DeriveMech_RawEncryptUnsafe`
- `DeriveMech_RawEncryptZeroPadUnsafe`
- `DeriveMech_PKCS8EncryptUnsafe`

These can be used in the same way as the `DeriveMech_RawEncrypt`, `DeriveMech_RawEncryptZeroPad` and `DeriveMech_PKCS8Encrypt` mechanisms (respectively). However, they will permit `Mech_RijndaelmGCM` to be specified.

In order to use a key-wrapping mechanism, a key must have an ACL (Access Control List) entry which gives the allowed DeriveKey mechanism in its mech field. Any keys currently held within a Security World will not mention the new `DeriveMech_RawEncryptUnsafe` mechanism. So they will continue to be prevented from using `Mech_RijndaelmGCM`, and will be protected from the same-IV attack.

In order to use the new mechanisms, therefore, it will be necessary to re-import the wrapping key into the Security World, whilst giving it an ACL which permits `DeriveMech_RawEncryptUnsafe` (etc.). Alternatively, if the key is "recoverable" within the Security World, its

ACL can be changed using authorization from the Admin Card Set. In other words, an explicit step is needed to confirm that each wrapping key can be used with user-supplied IVs; it is then the responsibility of the user to ensure that the same-IV attack above is effec tively mitigated.

These new mechanisms are not permitted in FIPS Level 3 Security World.

3.9. nShield Connect Tamper Changes

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

Changes have been made to the tamper responsiveness of the nShield Connect to comply with the certification requirements. Specifically this means:

- **nShield Connect Tamper events can no longer be disabled**.
- When a tamper event does occur on a nShield Connect or nShield 5c a factory reset occurs automatically with no user confirmation required.

3.10. nShield Connect CLI (Serial Console) Update

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

The nShield Connect XC Serial Console and the nShield 5c now support faster serial speeds (baud rate). By default the v13.3 Connect images will default to the 115200 baud rate but this can be downgraded to 9600, which was the speed used in previous releases. This option can be configured in the Connect configuration file or the Connect Front Panel UI.

For the Connect Configuration file the option is in the `Serial port configuration` section, where the line speed can be changed from 115200 to 9600.

3.11. IPv6 NTP support for nShield Connect

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

The nShield Connect has a NTP client that can be configured to support the synchroniza- tion of system time on the Connect with one or more NTP servers. In Security World v13.3 this NTP client on the nShield Connect has been updated to allow support NTP servers con figured with IPv6 addresses. When configuring the NTP client on the nShield Connect, the different IP addresses of the NTP servers can be supplied as IPv4 or IPv6 addresses.

3.12. Remote Admin Client support of IPv6

Impacts: Remote Admin Client

The Remote Admin Client has now been updated to support IPv6 addresses. The address of the Remote Admin Service can be either:

- IPv4 Address
- IPv6 Address
- Hostname

3.13. RFS Authentication

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

In previous releases of Security World, RFS clients can be authenticated by RFS servers, but RFS clients cannot authenticate RFS servers. In Security World v13.3 support was added to allow the server end of the RFS to be authenticated by RFS clients in all relevant configuration locations and RFS tools (using KNETI). In particular this allows an nShield Connect to be able to authenticate the RFS Server.

Consult the *Connect User guide* for further details.

3.14. Java 17 support

Impacts: clientside software

Support for Java 17 (both Oracle JDK and OpenJDK) has been added to the nCipherKM JCA/JCE Provider. Java 7 is no longer supported. The following versions of Java have been tested with, and are supported by, the nCipherKM Provider:

- Java 8
- Java 11
- Java 17

3.15. RedHat OS Support Updates

Impacts: clientside software

Support for the Red Hat Enterprise Linux 9 operating system has been added to Security World v13.3. This includes support for all supported HSM types (Edge, Solo+, Solo XC,

nShield 5s, Connect+, Connect XC and nShield 5c).

Previously the nFast installer would always use SysV `init` scripts and on systems using `systemd` this would be interpreted by its compatibility layer. Now the installer will check for systemd and write service files where this is so, and fall back to using SysV `init` scripts otherwise.

Support for RedHat 6 is no longer officially support. Support remains for RedHat 7 and Red Hat 8. See Compatibility for more details.

3.16. PKCS#11 Updates

Impacts: clientside software

The following has been added to the PKCS#11 library in the v13.3 release:

- Support for AES Counter Mode (Encrypt and Decrypt): `CKM_AES_CTR`
- Support for `CKA_COPYABLE` and `CKA_DESTROYABLE`
- PKCS#11 load sharing mode now supports object creation as well as standard crypto operation
- Support for faster EC/DH key exchange; a new vendor define attribute `CKA_NC_VALUE_ONLY` will provide faster key derivation operations when using loadsharing.

Consult the *PKCS#11 API Guide* for further information.

4. Security World v13.3 Notes

This section contains general notes of importance for the Security World v13.3 release.

4.1. nShield 5s and nShield 5c hardware

Security World v13.2 introduced support for the new nShield 5 HSM hardware (nShield 5s and nShield 5c), which was only used by customers using the new HSM hardware.

Security World v13.3 includes support for the new nShield 5 HSM as well as support for all other HSM types.

The nShield 5s and 5c have their own Installation and User guide which contain more information, however some detail about the main changes in nShield 5 hardware and features is listed below. Contact nshield.support@entrust.com for more information.

4.1.1. nShield 5s

The nShield 5s is a new HSM based on the 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

4.1.2. 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.

4.1.3. nShield 5 features

4.1.3.1. 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.

4.1.3.2. 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.

4.1.3.3. 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.

The host still uses `impath` to communicate with the nShield 5c.

4.1.3.4. nShield 5 limitations

At the time of release there are the following limitations of the nShield 5 product:

- 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. The CodeSafe developer product shipped as part of 13.3 does not contain any nShield 5 support and is for Solo XC and Solo+ only.

4.2. Firmware and nShield Connect ISO changes

The Firmware and nShield Connect ISO has been updated to improve the layout and naming of the firmware and Connect images.

nShield Firmware

The nShield HSM Firmware is still located inside the `firmware` directory on the ISO, however:

- The subdirectories are now named by HSM product type (i.e. `/firmware/SoloXC/` and `/firmware/nShield5s/`)
- Within each HSM product folder there is a further set of directories splitting up the firmware by its certification status (i.e. `latest`, `fips`, `cc`)
- The filename of the firmware files have been changed to contain (1) product HSM name, (2) version and (3) VSN (i.e. `soloxc-13-3-1-vsn37` and `soloxc-12-72-1-vsn37`)

When choosing a firmware, select the directory of the HSM of interest, then select the directory that matches the certification status, which will contain the required HSM firmware. So as example:

- Latest nShield 5s HSM firmware (v13.3.1) - `/firmware/nShield5s/latest/nshield5s-13-3-1-vsn2.npkg`

- Latest Solo XC HSM firmware (v13.3.1) - `/firmware/SoloXC/latest/soloxc-13-3-1-vsn37.nff`
- FIPS Certified Solo HSM firmware (v12.72.0) - `/firmware/Solo/fips/solo-12-72-0-vsn29.nff`
- FIPS Certified Edge HSM firmware (v12.72.0) - `/firmware/Edge/fips/solo-12-72-0-vsn29.nff`

nShield Connect Images

The nShield Connect images are still located inside the `nethsm-firmware` directory on the ISO, however:

- The subdirectories are now named by (1) certification status, (2) product supported by that image, (3) version number and (4) VSN, i.e. `latest-all-13-3-1-vsn32` and `cc-xc-13-3-1-vsn32`
  - The product support will usually state `all` to indicate that the Connect image supports all HSM types and contains a suitable firmware image that supports the required certification. However there are some Connect images that are just for specific Connects based on that certification just being on that HSM. In this case the product support can be `xc` for Connect XC, 'plus' for Connect+ or `nshield5c` for the nShield 5c.
- There is no change in the filename of the Connect image (continues to be `nCx3N.nff`)

When choosing a Connect image, select the directory that matches the Connect type and certification status. So as example:

- Latest Connect+ image (with v13.3.1 firmware) - `/nethsm-firmware/latest-all-13-3-2-vsn32/nCx3N.nff`
  - This Connect image supports all Connect types (Connect+, Connect XC and nShield 5c), so is listed as `all` under product support. This will upgrade the Connect image to v13.3.2 with the latest HSM firmware
- CC Connect XC image (with v12.60.15 firmware) - `/nethsm-firmware/cc-xc-13-3-2-vsn32/nCx3N.nff`
  - This Connect image is for Connect XC only, so product support is listed as `xc`. It will upgrade the Connect XC image to v13.3.2 with the 12.60.15 CC firmware
- FIPS nShield 5s image (with v13.2.2 firmware) - `/nethsm-firmware/fips-all-13-3-2-vsn32/nCx3N.nff`
  - There is a FIPS firmware for all HSM types, so this Connect image can be used on all nShield Connects. The Connect image will be upgraded to v13.3.2 with the relevant FIPS HSM firmware being included

4.3. Updated FIPS Firmware available

4.3.1. FIPS Security World mode rename

In previous Security World releases the Security World FIPS Level-3 mode was called `fips-140-2-level-3`, which reflected the FIPS 140-2 compliance of that Security World. With the introduction of the nShield 5s which now complies with FIPS 140-3, this Security World mode has been renamed to `fips-140-level-3`.

A summary of the available Security World modes is listed in the table below:

Security World mode designation	`new-world` **mode param**	**Description**
FIPS 140 Level 3	`fips-140-level-3`	This is the FIPS 140 level 3 approved mode of operation. Customers needing FIPS 140 Level 3 compliance can use this mode on an HSM with a FIPS validated firmware version.
Common Criteria CMTS	`common-criteria-cmts`	The Common Criteria approved mode of operation for Protection Profile EN 419 221-5 Cryptographic Module for Trust Services. Customers needing Common Criteria (CC) compliance can use this mode on an HSM with a CC validated firmware version.
Unrestricted	*unspecified*	The unrestricted Security World mode protects keys with FIPS approved crypto, but it is not designed to be fully compliant with all the requirements and restrictions of a particular certification standard. This mode can be used by customers who want their keys securely managed within the FIPS level 3 boundary, but don't need full compliance with the certification approved modes of operation. Note: for Solo XC, Solo+ and Edge, the unrestricted mode is compliant with FIPS 140-2 Level 2.

4.3.2. nShield 5s

The nShield 5s firmware from the v13.2 release is FIPS 140-3 Level 3 FIPS Pending. See https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List for the current FIPS queue.

FIPS certification is expected to complete in 2023. Contact nshield.support@entrust.com for the latest certification information. This firmware release is available in the v13.3 nShield Firmware ISO. A v13.3 nShield Connect image is available containing this FIPS firmware. See

HSM Firmware and nShield Connect images for details of the images.

4.3.3. nShield Edge, Solo+ and Solo XC

The Security World v13.3 nShield Firmware ISO contains an updated set of FIPS firmware that has been certified to FIPS 140-2 Level 2 and FIPS 140-2 Level 3 for the nShield Edge, Solo+ and Solo XC HSMs. These firmware releases contain new features and changes mandated by NIST as part of the FIPS standard. These changes are required for certification to be achieved and previous versions of firmware will move to the historical list at a time mandated by NIST. All of these changes are present in the latest v13.3 firmware as well.

An updated v13.3 nShield Connect image is available containing this new FIPS firmware. See HSM Firmware and nShield Connect images for details of the images.

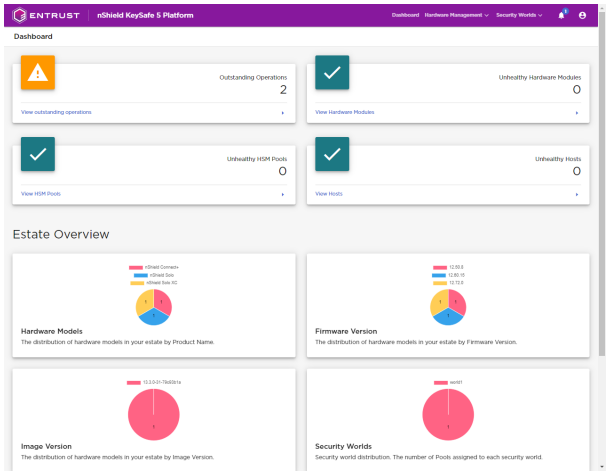
Please consult the *12.72 FIPS Firmware release notes* for more information regarding using this firmware release.

This relates to the following certificates:

HSM	Firmware Version	FIPS Level	Certificate	Security Policy
nShield Edge F2	v12.72.0	FIPS 140-2 Level 2	4331	Security Policy
nShield Edge F3	v12.72.0	FIPS 140-2 Level 3	4332	Security Policy
nShield Solo XC F2	v12.72.1	FIPS 140-2 Level 2	4333	Security Policy
nShield Solo XC F3 nShield Solo XC F3 for nShield Connect XC	v12.72.1	FIPS 140-2 Level 2	4334	Security Policy
nShield Solo XC F3 nShield Solo XC F3 for nShield Connect XC	v12.72.1	FIPS 140-2 Level 3	4335	Security Policy
nShield Solo+ F2	v12.72.0	FIPS 140-2 Level 2	4336	Security Policy
nShield Solo+ F3 nShield Solo+ F3 for nShield Connect+, Connect CLX	v12.72.0	FIPS 140-2 Level 2	4337	Security Policy

HSM	Firmware Version	FIPS Level	Certificate	Security Policy
nShield Solo+ F3 nShield Solo+ F3 for nShield Connect+, Connect CLX	v12.72.0	FIPS 140-2 Level 3	4338	Security Policy

4.4. KeySafe 5



nShield KeySafe 5 is a new nShield management platform that allows the management of an estate of HSMs through an intuitive web-based UI. The system also contains a RESTful API which can be used directly if required to provide custom management of the estate. KeySafe 5 supports the Security World v13.3 release and can be used to manage the Security World estate. Contact nshield.support@entrust.com for more information and access to this new product.

4.5. Notes for future releases

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

Preloading available only from preload utility

- The `with-nfast` utility is deprecated and will be removed in a future release. The `preload` utility should be used instead.
- The `--preload` parameter to the `ppmk` utility for preloading softcards is deprecated and to be removed in a future release. The `preload` utility should be used instead.

Solo+ and Connect+ Support

Security World v13.3 is the final Security World GA release providing updated **latest** firmware for the nShield Solo+ and **latest** images for the nShield Connect+ HSM. Support continues for released Solo+ firmware and Connect+ images. Future releases of clientside will continue to support Solo+ and Connect+ HSM versions from previously releases. This is following the announcement of the End of Life of the Solo+ and Connect+ HSMs. Contact nshield.support@entrust.com for further information.

5. HSM Firmware and nShield Connect images

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 ISO has been updated in v13.3, see Firmware and nShield Connect ISO changes for more information.

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

5.1. Firmware images

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	13.3.1	Latest firmware with features from v13.3 release.	`firmware/nShield5s/latest/nShield5s-13-3-1-vsn2.npkg`	2

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
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

Type	Version	Description	Directory	VSN
Latest	13.3.1	Latest firmware with features from v13.3 release.	`firmware/SoloXC/latest/soloxc-13-3-1-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-vsn29.nff`	29
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 v13.3 nShield Connect images that contain the Solo+, Solo XC and nShield 5s firmware described in Firmware images.

5.2.1. nShield 5c images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Pending	13.3.2	13.3 nShield Connect image with FIPS pending firmware	13.2.2	`nethsm-firmware/fips-all-13-3-2-vsn32/nCx3N.nff`	32
Latest	13.3.2	13.3 nShield Connect image with latest 13.3 firmware	13.3.1	`nethsm-firmware/latest-all-13-3-2-vsn32/nCx3N.nff`	32

5.2.2. 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
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-vsn-31/nCx3N.nff`	31
FIPS Approved	13.3.2	13.3 nShield Connect image with FIPS approved firmware	12.72.1	`nethsm-firmware/fips-all-13-3-2-vsn32/nCx3N.nff`	32
Latest	13.3.2	13.3 nShield Connect image with latest 13.3 firmware	13.3.1	`nethsm-firmware/latest-all-13-3-2-vsn32/nCx3N.nff`	32

5.2.3. nShield Connect+ images

5.2.3.1. 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 within a serial number ranges indicated below, Entrust advises against updating it to v13:

- `26-NC**`

- 28-NC**
- 36-NC**
- 37-NC**

Note that there is a VSN increase in the v13 image. If you upgrade the device, it is not possible to downgrade to an older image. If you upgrade, the Fan within the Fan Tray unit spins at its maximum rated RPM. However, this 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
FIPS Approved	13.3.2	13.3 nShield Connect image with FIPS approved firmware	12.72.0	nethsm-firmware/fips-all-13-3-2-vsn32/nCx3N.nff	32
Latest	13.3.2	13.3 nShield Connect image with latest 13.3 firmware	13.3.1	nethsm-firmware/latest-all-13-3-2-vsn32/nCx3N.nff	32

5.2.4. nShield Connect CLX images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	13.3.2	13.3 nShield Connect image with FIPS approved firmware	12.72.0	nethsm-firmware/fips-all-13-3-2-vsn32/nCx3N.nff	32
Latest	13.3.2	13.3 nShield Connect image with latest 13.3 firmware	13.3.1	nethsm-firmware/latest-all-13-3-2-vsn32/nCx3N.nff	32

6. Upgrade from previous releases

6.1. Security World Software upgrade

Before installing the v13.3 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 v13.3 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.

The VSN of the nShield Connect v13.3 image has been increased to 32. Increasing the VSN ensures that once the nShield Connect image file from v13.3 has been installed, it is only possible to upgrade to a Connect image with the same or a higher VSN. Downgrading to previous v12.80 or earlier Connect images will not be possible. Contact nshield.support@entrust.com if you required further information.

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 pro-

vided on the v13.3 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
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**

Operating System	Solo+	Solo XC	nShield 5s	Connect+, Connect XC, nShield 5c	Edge
Oracle Enterprise Linux 7 x64	Y	Y	Y	Y	Y
Oracle Enterprise Linux 8 x64	Y	Y	Y	Y	Y

Security World v13.3 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
3.8	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	N	N	Y	N
Microsoft Hyper-V Server 2019	N	Y	N	Y	N
Microsoft Hyper-V Server 2022	N	Y	N	Y	N

Operating System	Solo+	Solo XC	nShield 5s	Connect+, Connect XC, nShield 5c	Edge
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 v13.3 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. Option Pack support

Option Pack	Compatible Version
Web Services Option Pack (WSOP)	v3.1
Time Stamp Option Pack (TSOP)	Not yet released
Database Security Option Pack (nDSOP)	Not yet released
Cloud Integration Option Pack (CIOP)	v2.2.1
nShield Container Option Pack (nCOP)	Not yet released

Contact nshield.support@entrust.com for further information about the availability of any option pack.

9. Defect fixes

9.1. Defect fixes in clientside software

Reference	Description
NSE-53663	Fixed an nfpython issue where ACL construction can fail in some cases.
NSE-53052	Fixed an issue where the nShield Edge systemd service file was incorrectly marked as executable on Linux.
NSE-52874	Fixed an issue where the ncdate tool could crash when setting the HSM time fails.
NSE-50028	The metadata associated with Python wheels shipped with the product has been updated to have the latest wording.
NSE-48605	Fixed an issue where nShield 5 module enrollment could fail on non-English-language versions of Windows.
NSE-47080	Fixed an issue where an error about DynamicSlotExchangeAPDUs could appear in the hardserver log after clearing the module.
NSE-47048	It is now possible to use an nShield 5c as either the source or destination HSM when performing key migration.
NSE-46925	The hsmadmin keys backup command can no longer be used to write to a folder rather than an individual file. This prevents potential issues that could occur due to the folder permissions being altered.
NSE-46771	nethsmadmin error reporting fixed when attempting a firmware upgrade while the Connect RFS configuration is incorrect.
NSE-46592	Fixed an issue where the hardserver could fail start-up if a previously enrolled nShield 5 HSM was removed.
NSE-46182	An issue has been fixed that could have resulted in the error message 'TypeError: can only join an iterable' when performing key migration using the migrate-world command.
NSE-46101	An issue has been fixed that could have resulted in a stack trace if a non-existent ESN number was used in some hsmadmin commands.
NSE-46070	The speed rating displayed by the fet command has been corrected for all module types.
NSE-44909	Fixed an issue where the hardserver could fail an assertion when a device queue was maxed out in certain limited circumstances.
NSE-43384	An issue has been fixed that prevented a valid CSR from being created when using the nfwarrant command.
NSE-42778	The cfg-pushnethsm tool no longer requires IPv6 addresses to be enclosed in square brackets.

Reference	Description
NSE-42504	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-42370	The help text for the strict parameter to generatekey has been updated to reflect current behaviour.
NSE-42085	Fixed an issue where some error message strings in hardserver logs or in errors returned by the hardserver were incorrect.
NSE-42010	Update and clarify nethsmadmin help text and usage, in particular with regards to the RFS and authentication options. New warning messages thrown when these options are wrongfully specified.
NSE-41941	Fixed an issue where the firewall rule needed for the hsmadmin tool to detect nShield 5s modules was not set correctly in the Windows installer.
NSE-41857	Fixed an issue where the ncperftest tool could hang at start-up in some cases.
NSE-41850	Updated the start menu entry to include both the product family and the product name.
NSE-41847	rfs-sync utility authentication options updated. By default the software KNETI key is now used to authenticate to the RFS. The --authenticate option can be used to authenticate with a module KNETI key instead. The --no-authenticate option is deprecated.
NSE-41788	Fixed an issue where the wrong IV length was passed in the CodeSafe tickets example code.
NSE-41711	Fixed an issue where some required executables were included in the optional ctls (user tools) package rather than the hwsp (core hardware support) package.
NSE-41618	Update the tool to handle the correct combination of single or multiple arguments.
NSE-41567	Fixed an issue where nCipher CAPI (CryptoAPI) CSPs could fail with the errors "Existing-Client () failed: ClientUnknown" and "NFast_Present: Unable to get world info in NFast_Present" in some cases.
NSE-41497	API documentation for DeriveMech_AESKeyWrap, DeriveMech_AESKeyUnwrap and Mech_AESKeyWrapPadded were improved.
NSE-41401	The CNG provider will now generate ECDSA signatures of hashes longer than the curve order.
NSE-41351	During module initialization, module state certificates use KLF2 in all security world types. Formerly, legacy world types used the now-deprecated KLF.
NSE-41345	A segmentation violation in in the nShield pkcs#11 API C_UnwrapKey function caused by passing a NULL for the pTemplate[0].pValue value pointer has been fixed.
NSE-40428	The debug diagnostics for the nShield pkcs#11 API C_GetMechanismList function now print the correct slot id.
NSE-40198	API documentation for NFKM_NKF_RecoveryDisabled was improved.

Reference	Description
NSE-40186	API documentation for DSAComm, DSACommVariableSeed and DSACommFIPS186_3 was improved.
NSE-40180	Integrity mechanisms can be used with DeriveMech_RawDecrypt.
NSE-40174	Under certain circumstances the startup script for the hardserver would determine that the hardserver was already running and not attempt to start it. The detection mechanism has been updated to ensure that a correct determination of the hardserver running is made.
NSE-39862	Fixed an issue introduced in v12.70 where a hardserver client connection that continuously completely fills the HSM queues could prevent other connections from making progress with their commands.
NSE-39321	Codesafe for SoloXC was shipped with some incorrect header files, which were causing memory errors. These have now been fixed.
NSE-39289	The NFKM engine now supports the ECPrivate and ECPublic generic EC key types.
NSE-39155	Fixed an issue where the first few log messages from the nFast Server service were not written to the Windows Event Log.
NSE-39017	Fixed an issue where connections to the hardserver service could fail to be accepted if hundreds of simultaneous local or remote connections were attempted, due to default OS connection queue limits being applied. This could be an issue for example for highly multi-threaded applications during start-up. The maximum number of simultaneous connection attempts supported is now 10,000 (where the OS supports this). Note that this is separate from the number of total connections that can be open at once overall, which can be much higher still.
NSE-37892	The nShield pkcs#11 library no longer sets ExportAsPlain for keys generated in CMTS worlds.
NSE-37856	Improved performance for nfkmcheck
NSE-37854	nfkmverify -v now prints full public keys, as documented.
NSE-37365	ck_ecedwards_gen, cknfkmid, and ckcrypt are now included in the PKCS11 examples
NSE-37101	nShield service users and groups on Linux are now created in the system ID range, and nShield service users are created with a nologin shell specified. These changes apply to newly created users and groups; if you wish to recreate existing entities, delete them and then re-install the nShield software. Note that if you downgrade to older versions of nShield after creating users with the nologin shell, you will either need to modify the service user shell to sh or bash or delete the users and let the nShield install script recreate them.
NSE-35564	Excessively strict validation of enumeration types in nfpython was relaxed.
NSE-35407	API documentation for ECDSA and KCDSA signature mechanisms was improved.
NSE-35209	M_StatID validation was relaxed, in order to address issues with mixed-version deployments.
NSE-34786	Timestamps have now been added to the raclient debug logs.

Reference	Description
NSE-34133	The help text for the --use-kneti parameter to cfg-pushnethsm has been updated to clarify that it should only be used when using an nToken or local HSM KNETI key to authenticate, and that that parameter should be omitted when using the default hardserver software KNETI authentication key.
NSE-34008	Fixed an issue where the PowerShell Add-nShieldToProfile command would fail if the Power Shell profile directory for the user was not present.
NSE-33878	Issue fixed where nfkmverify reports "unexpected derivekey mechanism" for the AESKey-Wrap, AESKeyUnwrap and NISTKDFmCTRpRijndaelCMACr32 derive mechanisms.
NSE-33750	The ckmechinfo utility has been updated to display correct names.
NSE-32441	Fixed an issue where card-loading (e.g cardpp, createocs, new-world) could hang when there were unused gaps in module or slot numbers.
NSE-30360	An issue where nfkmverify could crash was fixed.
NSE-28883	The mechanism for determining if systemd is running has been updated.
NSE-28534	Multiple NIST and other specification references were added to nCore API documentation.
NSE-27594	Obsolete PCIe Exard drivers, and all supporting references, have been removed from the Linux Security World ISO.
NSE-26863	Fixed an issue where nShield Edge device enumeration could fail on Windows, resulting in the modules not being available unless specified explicitly in the config file by their COM port. This especially affected cases where more than one nShield Edge device was used.
NSE-25518	rfs-sync description in the Supplied Utilities section of the Connect User Guide corrected. The rfs-sync utility shall be run on a client and not the RFS.
NSE-25477	The option to set the nShield CSPs as the default SChannel CSPs has been removed to prevent users from being unable to log in following a reboot of the machine. If the nShield CSPs are set as the default, it will be necessary to enter safe mode and then remove the nShield CSPs as the default SChannel CSPs.
NSE-15163	The nCipher MIB has had minor updates to fix issues reported by some monitoring tools. It is recommonded to copy the new mib file to any system that needs it.
NSE-12560	Fixed an issue where an enrolled Connect could sometimes remain incorrectly failed with ServerAccessDenied after recovery from a connection failure or Connect reboot.

Reference	Description
NSE-11239	A restriction has been added to the permitted paths that can be shared as RFS (Remote File System) volumes. NFAST_KMDATA (/opt/nfast/kmdata on Linux or "C:\ProgramData\nCipher\Key Management Data" by default on Windows) is one of the paths that are permitted by default. Subdirectories of permitted paths are also permitted. In addition, any paths associated with RFS volumes created by the rfs-setup utility are permitted by default. If custom paths are added as RFS volumes they must be added to the allow-list explicitly before starting the hardserver (nFast Server) service either by setting the NFSERV_RFS_ALLOWED_PATHS environment variable or by creating a config.secure JSON file specifying the "rfs_allowed_paths" key. See the User Guide for more information about these configuration options if custom paths are being shared as RFS volumes.
NSE-6661	Fix to the Linux install script for nShield Edge to not error on missing ftdi_sio and to list as warning to allow the install script to complete.
NSE-4112	Fixed an issue where Ctrl-C and Ctrl-Z were not supported to terminate or suspend the process during passphrase prompts in the ppmk and cksotool applications on Linux.
NSE-1676	Fixed an issue where the nShield installer on Linux only checked local user and group databases before attempting to create missing entities. The install script now uses the getent tool if it is available in order to take account of users and groups managed by alternate user/group databases such as LDAP.

9.2. Defect fixes in Solo+, Solo XC, and nShield 5s firmware

Reference	Description
NSE-51190	It is now possible to apply features to an nShield 5 module using a smart card. Previously it was only possible to apply upgrades via a certificate file or the keyboard.
NSE-43807	Certain pathological elliptic curve cryptography domains which could have been incorrectly accepted are now rejected.
NSE-43515	In Mech_ElGamal, ephemeral private keys are now the same size as the modulus p, to mitigate the risk of bad group choices by non-nShield peers.
NSE-42346	Fixed an issue where nShield Edge was not supported if there were also nShield PCIe devices installed.
NSE-42034	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-41139	Validation of elliptic curve cryptography domains was tightened to reject additional pathological cases.
NSE-40017	A missing self-test was enabled.
NSE-39505	API documentation for the SupportsAuthentication flag was corrected.

Reference	Description
NSE-37311	The minimum embedding degree of custom elliptic curve domains was increased to 100, in line with FIPS requirements.
NSE-34754	Policy checking on elliptic curve cryptography domains was made more independent of rep resentation..
NSE-33382	DeriveMech_HyperledgerClient was extended to support KeyType_ECPrivate, in line with other ECC mechanisms.
NSE-23250	Fixed an issue in the Solo XC RTC to prevent it from loosing time following a cold restart.
NSE-28524	Fixed an issue in the Solo XC RTC to prevent it from loosing time following a restart of the hardserver.

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

Reference	Description
NSE-47043	Fixed issue in the FPUI menus where the RFS configuration is not properly reloaded when updated via a different interface (i.e. serial CLI command, or config file push/fetch).
NSE-46991	Reducing number of retry attempts and delay each time round when the Connect cannot transfer its configuration file to the RFS (e.g. if the RFS configuration is incorrect).
NSE-46962	Verifying key ACLs via the nShield5c's FPUI isn't currently possible.
NSE-46752	The nShield 5c system time cannot be set via its CLI. It can only be set via the front panel or NTP.
NSE-46222	nShield 5c CLI netcfg command won't display correct network information.
NSE-43411	Fixed an issue where initialization of client hardserver connection to nShield Connect can timeout in client when the system is under load.
NSE-42578	Fixed a typo in the time displayed on the front panel user interface of the nShield Connect. The time is now shown as hh:mm:ss, instead of hh.mm:ss.
NSE-42486	Fix the value of the minimum temperature of the security processor, as shown on the nShield Connect front panel user interface. The format did not work with negative numbers, but now does.
NSE-41968	Fixed an issue which could cause the hardserver to abort.
NSE-41620	The default impath_resilience_timeout was previously 1 week; the default timeout has now been changed to 1 hour.
NSE-40445	The IPv6 traceroute option on netui (1-1-1-8-2) is now consistent with the IPv6 ping menu in that, for IPv6 link-local addresses, the same interface selection sub menu (giving options for either Interface #1 or Interface #2) is displayed upon entering a fe80 prefixed address

Reference	Description
NSE-34754	Policy checking on elliptic curve cryptography domains was made more independent of rep resentation.
NSE-33382	DeriveMech_HyperledgerClient was extended to support KeyType_ECPrivate, in line with other ECC mechanisms.
NSE-43575	Fixed an issue where when pressing "Back" on the front panel on the Client Configuration screen did not actually go back.

10. Known issues in Security World 13.3

See also Known issues from earlier Security World releases.

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 Upgrades from Previous releases section 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.

11. Known issues from earlier Security World releases

These issues are still present in v13.3.

Reference	Description
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. This mode changes the settings for the nShield Connect firewall so that it will pass-through packets which are discarded in the normal Default mode. This behaviour is required for compliance testing but is not recommended for normal use since allowing packets with invalid fields or parameters through the firewall increases the attack surface. This mode is known not to function correctly in the v12.80 Connect Image and should not be enabled.
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	nCipher Security 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 Wold then it is not possibly to verify OCS and softcard protected keys directly with nfkmverify. The OCS or softcards must be preloaded prior to attempting to verify the keys.
NSE-24335	Note: 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.

Reference	Description
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.
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.