Release Notes

nShield Security World v13.6.5 Release Notes

Table of Contents

1. Introduction . . . 1
    1.1. Updated nShield Software Release Policy . . . 1
    1.2. Purpose of Security World v13.6 . . . 1
    1.3. Versions of these Release Notes . . . 2
2. Product versions . . . 5
    2.1. Security World software versions . . . 5
    2.2. CodeSafe Developer software versions . . . 5
    2.3. Firmware and Connect ISO versions . . . 5
    2.4. nShield Firmware versions . . . 5
    2.5. Connect image versions . . . 5
3. Updates in v13.6.5 Release . . . 7
    3.1. Defect Fixes . . . 7
    3.2. Updated nShield 5s FIPS firmware . . . 7
    3.3. Open Source Software Updates in the 13.6.5 release . . . 7
        3.3.1. Security World Software . . . 7
        3.3.2. Security World Software Python Packages . . . 7
        3.3.3. Codesafe 5 . . . 8
        3.3.4. nShield Connect XC and nShield 5c . . . 8
        3.3.5. Remote Administration Client . . . 9
        3.3.6. Python Zlib . . . 9
4. Features of Security World v13.6 . . . 11
    4.1. nShield 5s Common Criteria Certification . . . 11
    4.2. Updated FIPS 140-3 nShield 5s, 140-2 Solo XC and Edge Firmware . . . 11
    4.3. FIPS Certificates . . . 12
    4.4. Connect XC and 5c client licensing now restricted by connection count (NSE-29138) . . . 13
    4.5. Signed System Logs (NSE-46881) . . . 13
    4.6. New Audit logging implementation (NSE-42926, NSE-55878, NSE-55935) . . . 14
    4.7. Connect XC and 5c remote administration (NSE-55295) . . . 15
    4.8. Updated Open Source Software used in Security World Software (NSE-55465) . . . 15
    4.9. Visual Studio 2022 Support (NSE-24350) . . . 16
    4.10. Generic SP800-108 KDF (NSE-50408) . . . 16
    4.11. Ed448 support in firmware (NSE-51255) . . . 16
    4.12. RFC5869 HKDF in firmware (NSE-49151) . . . 17
    4.13. Attestation of system keys (NSE-49689) . . . 17
    4.14. ECC is now enabled by default (NSE-48784) . . . 17

4.15. Updated nShield 5s Bootloader (NSE-48712) . . . 18
4.16. Network status is now exposed via Stattree (NSE-53969) . . . 18
4.17. Network interfaces are now monitored on the Connect using SNMP . . . 18
4.18. Preload is now ported to Python 3 (NSE-38309) . . . 18
4.19. Updated nShield Remote Admin Client (NSE-38313) . . . 18
4.20. ACL analyzer for key attestation (NSE-55514) . . . 19
4.21. NFKM engine now permits asymmetric verification (NSE-39432) . . . 19
4.22. x931 support for NFKM engine (NSE-39304) . . . 19
4.23. nShield PKCS#11 library now supports v3 CKM_SP800_108_COUNTER_KDF (NSE-35939) . . . 19
4.24. Support for UNIX domain sockets on Windows (NSE-58561) . . . 20
4.25. CodeSafe changes for Solo XC and Connect XC . . . 20
4.25.1. CodeSafe fixes in Solo XC Firmware . . . 20
4.25.2. CodeSafe Host-side Fixes . . . 21
4.25.3. CodeSafe Developer Software Fixes and Improvements . . . 23
5. Firmware images . . . 27
5.1. nShield 5s firmware . . . 27
5.1.1. nShield 5s primary firmware . . . 27
5.1.2. nShield 5s Recovery image . . . 28
5.1.3. nShield 5s Bootloader . . . 28
5.2. Solo XC firmware . . . 29
5.3. nShield Solo+ firmware . . . 29
5.4. nShield Edge Firmware . . . 29
6. Connect images . . . 30
6.1. Install a Connect image . . . 30
6.2. nShield 5c images . . . 30
6.3. Connect XC images . . . 31
6.4. Connect+ images . . . 31
6.5. Connect CLX images . . . 31
7. Upgrade from previous releases . . . 32
7.1. Install 13.6.5 Security World Software . . . 32
7.2. Upgrade Solo XC firmware . . . 32
7.3. Upgrade nShield 5s HSM Firmware . . . 32
7.3.1. nShield 5s Firmware Version Check . . . 33
7.3.2. Upgrading the nShield 5s Primary & Recovery Image . . . 33
7.3.3. Upgrading the nShield 5s Bootloader . . . 34
7.3.4. nShield 5s VSN . . . 34
7.4. Upgrade a Connect XC image . . . 35
8. Compatibility . . . 36

8.1. Supported hardware . . . 36
8.2. Supported operating systems . . . 36
8.3. API support . . . 37
8.3.1. Java . . . 37
8.3.2. Python . . . 37
8.4. Supported hypervisors and virtual environments . . . 37
8.5. Supported compilers for Microsoft Windows C developers . . . 38
8.6. Option Pack support . . . 38
9. Documentation updates . . . 39
10. Known and fixed issues . . . 41

1. Introduction

These release notes apply to the release of version 13.6.5 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.

1.2. Purpose of Security World v13.6

Security World version v13.6 introduces new features and enhancements as described in Features of Security World v13.6. It also corrects a number of defects that have been identified in earlier releases.

Security World v13.6 is a **Long-Term Supported (LTS)** release. Updated releases will be made to this release adding enhancements and fixes as detailed in the Release policy. These improvements will be captured in these release notes.
See the nShield Security World Release Information for details of the supported versions and the support dates.

This release contains updates to the following products:

- Security World Software
- Updated firmware for nShield 5s and Solo XC
- Updated Connect images for nShield 5c and Connect XC
- CodeSafe Developer Software

This version of Security World uses two different version numbers for the above products:

- v13.6 - Security World Software and Connect images
- v13.5 - nShield 5s and Solo XC firmware

1.3. Versions of these Release Notes

Revision	Date	Description
3.1	2024-11-5	Updated release notes with: • Dedicated section for new 13.6.5 release containing additional details of changes. • Update to Purpose of Security World v13.6 section to list v13.6 as the LTS release. • Fix to include Go as an OSS update in 13.6.5. • New Option Pack support section detailing option packs supported with v13.6 release. • Updated FIPS Certificates table showing full details of certified versions. User guide updates: • Removed erroneous install location for CodeSafe 5 • Improved the description of hypervisor support
3.0	2024-10-25	Updated release notes for 13.6.5 LTS1 release
2.0	2024-09-26	Included NSE-58846 as a defect fix in the v13.6.1 Connect image Corrected a typo in the description of RSA PKCS#1 SHA-1 signature

Revision	Date	Description
1.9	2024-09-11	No changes to the product, documentation changes to clarify: • The need to add the `nfast\bin` directory to the Windows path • What the latest IEC/EN specification is • That on Linux installation is generally only supported in `/opt/nfast` • OCS time-out information about what happens with dynamic slots • Virtualization support in the HSM User Guide (the topic was erroneously removed in earlier v13.6.x document sets) • That elliptic curve support on Edge works on both Windows and Linux • The change in terminology from *whitelist* to *allowlist* • Uppercase/lowercase usage in SNPM node names
1.8	2024-08-28	No changes to the product, documentation changes to clarify: • The usage of `module_ESN_HKML` • That the CSP wizard doesn't create a security world • How many network-attached HSMs can be enrolled in a Security World as remote HSMs • When users need to run `hsc_configurepoolmodule` after enrolling a network-attached HSM to a security world
1.7	2024-08-14	Documentation changes only, no change to the product: • Corrected the supported Visual Studio version from 2017 to 2022 in the *PKCS #11 API Guide* • Fixed typos in the *Key Structures* chapter of the *nCore Developer Tutorial*
1.6	2024-07-31	Documentation changes only, no change to the product: • Corrected typos in Connect XC images: FIPS compliance is Approved for firmware 12.72.3, Common Criteria firmware version is 12.60.15 (*Release Notes*) • Updated the description of `rfs-setup` and `stattree` (*Utilities Guide*) • Updated the instructions to remotely load and update SEE machines and added that port 2205 has to be enabled between the RFS and the network-attached HSM for `csadmin` (*CodeSafe Guide*) • Added security advice about the use of `CKA_SENSITIVE=TRUE` in templates (PKCS #11 Guide) • Moved the SNMP information into its own guide in the API document set (*nShield SNMP Monitor v13.6.5 Install and User Guide*) • Added a troubleshooting item about frozen command-line to network-attached HSMs (HSM User Guide) • Fixed website link to the PDF of the *nShield Security World Software v13.6.5 Installation Guide*

Revision	Date	Description
1.5	2024-07-08	Addition of information about Common Criteria certified 5s firmware including primary and uboot updates added to Firmware images. Addition of information about the nShield 5s minVSN functionality added to nShield 5s VSN. Addition of information about documentation restructuring added to Documentation updates.
1.4	2024-07-05	Version for website publication. No content changes.
1.3	2024-07-03	Added note that HSM Pool mode is not supported with audit logging Security Worlds.
1.2	2024-07-02	Added fixed issues NSE-3946, NSE-50692, and NSE-60956.
1.1	2024-07-01	Note added to the description of NSE-48784: ECCMQV is available for Solo XC only. Clarification in HSM variant names.
1.0	2024-06-28	Security World v13.6 GA release notes.

2. Product versions

2.1. Security World software versions

Version	Date	Description
v13.6.5	2024-10-23	LTS1 release of 13.6.5 Security World Software.
v13.6.3	2024-06-26	First release of 13.6.3 Security World Software.

2.2. CodeSafe Developer software versions

Version	Date	Description
v13.6.5	2024-10-23	LTS1 release of 13.6.5 CodeSafe Developer software.
v13.6.3	2024-06-26	First release of 13.6 CodeSafe Developer software.

2.3. Firmware and Connect ISO versions

Version	Date	Description
v13.6.5	2024-10-23	LTS1 release of 13.6 Firmware and Connect ISO, including the release of firmware (13.5) and Connect image (13.6) along with FIPS and CC approved firmware and Connect images.
v13.6.3	2024-06-26	First release of 13.6 Firmware and Connect ISO, including the release of firmware (13.5) and Connect image (13.6) along with FIPS and CC approved firmware and Connect images.

2.4. nShield Firmware versions

Version	Date	Description
v13.5.1	2024-06-26	First release of 13.5.1 Firmware for nShield 5s HSMs containing the latest features and fixes.
v13.5.3	2024-06-26	First release of 13.5.3 Firmware for Solo XC HSMs containing the latest features and fixes.

2.5. Connect image versions

Version	Date	Description
v13.6.5	2024-10-23	LTS1 release of Connect images for 13.6 containing the latest features and fixes. Supersedes previous 13.6.1 release.
v13.6.1	2024-06-26	First release of Connect images for 13.6 containing the latest features and fixes.

3. Updates in v13.6.5 Release

The v13.6.5 release is a LTS update release which contains a number of improvements on top of the features introduced in the original release of v13.6, detailed in Features of Security World v13.6. These improvements are detailed below.

3.1. Defect Fixes

A number of defect fixes have been included in the v13.6.5 release. See Known and fixed issues for the complete list of defects fixed in the v13.6.5 release.

3.2. Updated nShield 5s FIPS firmware

The v13.6.5 release includes the complete set of updated firmware for the nShield 5s FIPS certifications, including the update nShield 5s Recovery image. See Firmware images for more details.

The updated 13.6.5 nShield 5c image contains the correct FIPS nShield 5s images for both Primary and Recovery ensuring that the nShield 5s firmware is in a valid FIPS configuration.

3.3. Open Source Software Updates in the 13.6.5 release

The following Open Source components have been updated as part of the 13.6.5 release:

3.3.1. Security World Software

OSS Name	13.6.3	13.6.5 LTS1
openssl	3.0.13	3.0.15
python	3.11.6	3.11.9
Go	1.21.9	1.22.5

3.3.2. Security World Software Python Packages

OSS Name	13.6.3	13.6.5 LTS1
certifi	2023.7.22	2024.8.30
cryptography	42.0.5	43.0.1

OSS Name	13.6.3	13.6.5 LTS1
idna	3.7	3.10
libpng	1.5.13	1.6.37
libtiff	4.2.0	4.7.0
paramiko	3.4.0	3.4.1
pip (nShield Python)*	23.2	23.2
pip (cpython)*	24.0	24.0
pip (virtualenv)*	24.2	24.2
pydantic	1.10.13	1.10.15
pyproject-hooks	1.0.0	1.1.0
requests	2.31.0	2.32.3
setuptools (nShield Python)**	68.2.2	73.0.0
setuptools (virtualenv)**	68.0.0	75.1.0
urllib3	2.07	2.2.3

*The 13.6.5 LTS1 nShield Python contains more than one version of the pip package. The pip package labelled with nShield Python is the one used primarily by the 13.6.5 LTS1 nShield Python build, unless the other packages are directly used.

**The 13.6.5 LTS1 nShield Python contains more than one version of the setuptools package. The setuptools package labelled with nShield Python is the one primarily used by the 13.6.5 LTS1 nShield Python build, unless the other packages are directly used.

3.3.3. Codesafe 5

OSS Name	13.6.3	13.6.5 LTS1
openssl	3.0.13	3.0.15

3.3.4. nShield Connect XC and nShield 5c

OSS Name	13.6.3	13.6.5 LTS1
libzlib	1.2.13	1.3.1
openssl	3.0.10	3.0.14
pip (nShield Connect)*	23.3.2	23.3.2

OSS Name	13.6.3	13.6.5 LTS1
pip (cpython)*	24.0	24.0
pip (virtualenv)*	23.3.1	23.3.1
python	3.11.2	3.11.9
setuptools (nShield Connect)**	68.2.2	73.0.0
setuptools (cpython)**	65.0.0	65.0.0
setuptools (virtualenv)**	68.0.0	68.0.0

*The 13.6.5 LTS1 nShield Connect contains more than one version of the pip package. The pip package labelled with nShield Connect is the one used primarily by the 13.6.5 LTS1 nShield Connect build, unless the other packages are directly used.

**The 13.6.5 LTS1 nShield Connect contains more than one version of the setuptools package. The setuptools package labelled with nShield Connect is the one primarily used by the 13.6.5 LTS1 nShield Connect build, unless the other packages are directly used.

3.3.5. Remote Administration Client

OSS Name	13.6.3	13.6.5 LTS1
certifi	2023.7.22	2024.8.30
idna	3.7	3.10
libpng	1.5.13	1.6.37
libtiff	4.2.0	4.7.0
python	3.11.6	3.11.9
requests	2.31.0	2.32.3
urllib3	2.0.7	2.2.3

3.3.6. Python Zlib

The Linux nShield Security World Software Python build uses the Zlib runtime on the host machine to run, this can be identified by executing 'zlib.ZLIB_RUNTIME_VERSION' in a Python shell. For build headers, the Linux nShield Security World Software Python will have used the Zlib on the build machine, this is slightly older but has no functional changes, this version may display as older than the runtime version.

Please refer to the Open Source document on the shipped ISO files for a full list of Open

Source in the product.

4. Features of Security World v13.6

4.1. nShield 5s Common Criteria Certification

The nShield 5s is now certified to the Common Criteria certification.

nShield 5s v13.5.1 is certified according to the Common Criteria v3.1Rev5 standard at EAL4+ augmented with ALC_FLR.2 and AVA_VAN.5, against the requirements in EN 419 221-5:2018, Protection Profiles for TSP Cryptographic Modules – Part 5 Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020. The Common Criteria certificate of nShield 5s v13.5.1 is issued by the Dutch NSCIB under reference NSCIB-CC-2200057-01, and it can be downloaded here https://trustcb.com/download/?wpdmdl=4019. Further inks to the CC Certification Report https://trustcb.com/download/?wpdmdl=4207 and Security Target https://trustcb.com/download/?wpdmdl=4208.

Leveraging the Common Criteria certificate, nShield 5s v13.5.1 also achieved the eIDAS approval as a Type 1 Qualified Signature/Seal Creation Device (QSCD) under reference eIDAS-2200058-01 (link here https://trustcb.com/download/?wpdmdl=4209) and is publicly listed at https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd.

Security World v13.6 provides a nShield 5c image, v13.6.1, which contains this certified v13.5.1 nShield 5s firmware.

4.2. Updated FIPS 140-3 nShield 5s, 140-2 Solo XC and Edge Firmware

Security World 13.6.5 includes updated versions of FIPS 140-2 Certified 12.72 firmware for the Solo XC and nShield Edge and updated FIPS 140-3 certified 13.2 and 13.4 firmware for nShield 5s.

Previous FIPS approved versions of Solo XC (v12.72.1) and nShield Edge (v12.72.0) nShield firmware remain FIPS approved and will continue to remain FIPS approved even when the new versions are certified. Upgrading to the latest versions of nShield firmware is only required if access to the latest changes in the nShield firmware are required.

The release notes for the specific firmware release (v12.72, v13.2 or v13.4) contain further information about the changes made as part of that release. For access to release notes from prior releases please

> contact https://nshieldsupport.entrust.com.

4.3. FIPS Certificates

Security World v13.6 supports all the currently active FIPS certified firmware versions including the newly certified nShield 5s v13.4.5 and v13.2.4 firmware. The table below lists these versions for each HSM. Consult the specific version release note for more information about that HSM firmware.

HSM	Certified Release	Version Info	FIPS Level	Certificate	Security Policy
nShield 5s	v13.4	• primary-version: 13.4.5 • recovery-version: 13.2.4 • uboot-version: 1.1.0	FIPS 140-3 Level 3	4765	Security Policy
nShield 5s	v13.2	• primary-version: 13.2.4 • recovery-version: 13.2.4 • uboot-version: 1.1.0	FIPS 140-3 Level 3	4745	Security Policy
Edge F2	v12.72	• 12.72.0 • 12.72.2	FIPS 140-2 Level 2	4331	Security Policy
Edge F3	v12.72	• 12.72.0 • 12.72.2	FIPS 140-2 Level 3	4332	Security Policy
Solo XC F2	v12.72	• 12.72.1 • 12.72.3	FIPS 140-2 Level 2	4333	Security Policy
Solo XC F3 Solo XC F3 for Connect XC HSMi	v12.72	• 12.72.1 • 12.72.3	FIPS 140-2 Level 2	4334	Security Policy
Solo XC F3 Solo XC F3 for Connect XC HSMi	v12.72	• 12.72.1 • 12.72.3	FIPS 140-2 Level 3	4335	Security Policy
nShield Solo+ F2	v12.72	• v12.72.0	FIPS 140-2 Level 2	4336	Security Policy
nShield Solo+ F3 nShield Solo+ F3 for Connect+, Connect CLX	v12.72	• v12.72.0	FIPS 140-2 Level 2	4337	Security Policy

HSM	Certified Release	Version Info	FIPS Level	Certificate	Security Policy
nShield Solo+ F3 nShield Solo+ F3 for Connect+, Connect CLX	v12.72	• v12.72.0	FIPS 140-2 Level 3	4338	Security Policy

4.4. Connect XC and 5c client licensing now restricted by connection count (NSE-29138)

The license model for Connect XC and 5c has been changed to enforce the licensed client count based on the number of concurrent client connections rather than the number of permitted clients in the configuration file.

This only applies to connections representing a normal unprivileged or privileged cryptographic client that been added with `nethsmenroll` or using the `[nethsm_imports]` configuration section. Connections for any RFS or config-push operations are not included. A client machine represents only a single licensed connection in this context, regardless of how many concurrent applications are running on that machine.

This means that more clients than are licensed may be configured, if some clients are not running all the time. It also means that clients which share an identity (same IP address behind NAT and/or same KNETI authentication key) will now be distinguished as separate concurrent clients and each will require a license. Such shared-identity clients are now also supported for session resumption (also referred to as Impath resilience or parked sessions) so that all clients behind NAT, for example, are able to resume their session successfully after a brief loss of network connectivity, without the need to re-load application keys.

4.5. Signed System Logs (NSE-46881)

The nShield 5s and nShield 5c HSMs loaded with firmware version 13.5 or later can now sign and export system logs generated by the HSM. These logs include system events such as the HSM booting up, periodic self tests, firmware upgrades and other administrator actions, system errors, etc.

It is recommended to save and clear the system logs immediately prior to upgrade to v13.5 firmware.

In order to generate a certificate that will protect the log signing key you should factory state your nShield 5s or nShield 5c HSM immediately after upgrading to v13.5 firmware.

4.6. New Audit logging implementation (NSE-42926, NSE-55878, NSE-55935)

HSMs loaded with firmware version 13.5 or later implement new protocols for signed audit-log generation that requires new configuration in the host-side software.

There are two types of audit-log generated by the HSM:

- nCore logs for certain cryptographic operations when enrolled in a Security World with audit-logging enabled.
- Signed syslogs (system logs) for system activity on the nShield 5s and nShield 5c (not the SoloXC or ConnectXC). This applies regardless of whether an audit-logging Security World is enabled.

Audit-logs need to be retrieved and deleted from the HSM via the new nShield Audit Log Service which is present in the Security World Software. The nShield Audit Log Service must be explicitly configured to specify the modules for which it is responsible for log fetching.

If the nShield Audit Log Service is not configured to retrieve and delete audit-logs from an HSM, then the HSM may exhaust its file system disk space and not run correctly until its audit-logs have been retrieved.

When configuring for ConnectXC and 5c, take care to configure only a single nShield Audit Log Service to fetch the logs for any given HSM. The client machine must be configured as a privileged client of the HSM, or be an RFS which is permitted to operate as a privileged client.

Retrieved audit-logs are saved in databases on the host machine where the nShield Audit Log Service is running. The audit-log databases can be queried and managed using the new `nshieldaudit` command-line tool. Consult the *nShield v13.6.5 HSM User Guide* for more information about configuration of the service and use of the client tool.

If you have a mix of HSMs with firmware before and after 13.5 with audit-logging Security Worlds loaded, you will receive nCore audit logs in both old and new formats. These logs are essentially independent and you must manage them separately. Configuration of the old "CEF" format nCore audit logging for previous firmware versions is unchanged, but a new tool `cef-audit-verify` is provided in the v13.6.5 Security World release to verify these logs, replacing the old `audit-log-verifier.py` example script.

HSM Pool mode keys are not supported by the new audit logging implementation. HSM Pool mode can be used only with Security Worlds which do not have audit logging enabled when using v13.5 firmware or

later.

4.7. Connect XC and 5c remote administration (NSE-55295)

v13.2 introduced support for the configured RFS machine (`[rfs_client]` section in the Connect XC or 5c config file) to be permitted automatically as a config-push client if authenticated (in addition to whatever push client was specified in the `[config_op]` configuration). This configuration applied by default when the RFS was authenticated (i.e. the configuration specified the hash of the KNETI authentication key of the RFS), but could be explicitly enabled by setting `push=ON` in the `[rfs_client]` configuration even if the RFS was not authenticated, or this feature explicitly disabled with `push=OFF`.

v13.6 extends this behaviour so that the configured RFS of a Connect XC or 5c is also permitted as a privileged client, in the same cases as it was previously allowed as a config-push client as explained above.

These changes reflect that certain administration operations such as pushing config files, or initiating upgrades or applying feature files remotely using the `nethsmadmin` utility, often involve the RFS, which may not necessarily be one of the machines configured as a normal client for cryptographic applications. The new nShield Audit Log Service also must be configured on a privileged client now, and the RFS is a natural choice for the machine to be designated that role.

A new tool `appliance-cli` has been added which supports some additional commands for administration of XC and 5c devices, which can be run from a privileged client. Run `appliance-cli -m1` (replace `1` with actual Connect XC or 5c module number) in order to see the available commands. The HSM logs-related commands are used automatically by the nShield Audit Log Service and so should not normally be needed directly, but this interface adds some other facilities including retrieving statistics information from the 5s HSM inside a 5c appliance, and also support for fetching the current state of the Connect XC or 5c config file on demand (`appliance-cli -m1 getservcfg --cfg config`). Additional commands may be added in future.

The new client licensing in v13.6 permits an additional free-of-charge privileged client license in recognition of use of the RFS as an administration client for these various use cases.

4.8. Updated Open Source Software used in Security World Software (NSE-55465)

The Open Source Software used in Security World Software has been updated to include newer versions to address Common Vulnerabilities and Exposures. For a detailed list of Open Source Software versions, please consult the `*-licenses.pdf` file on the ISO.

The following updates are of specific note:

- Python 2 has been removed from Security World Software and has been replaced completely with Python 3. All python Security World tools have been updated use Python 3. The version shipped with Security World v13.6 is version 3.11.6.
- The OpenSSL version has been updated from 1.1.1 to 3.0.13.

4.9. Visual Studio 2022 Support (NSE-24350)

nShield Security World software v13.6 has been updated to support Visual Studio 2022. This enables the development of applications against Security World Software APIs using the Visual Studio 2022 SDK.

4.10. Generic SP800-108 KDF (NSE-50408)

A new mechanism, `DeriveMech NISTKDFmGeneric`, has been added to support a range of NIST SP800-108r1 KDF variants, including the RFC5869 HKDF.

4.11. Ed448 support in firmware (NSE-51255)

Security World v13.6 introduces the Edward curve-448 digital signature algorithm (EdDSA) with the inclusion of two nCore mechanisms: Ed448 and Ed448ph.

Ed448ph Mechanism:

- Introducing the Ed448-with-prehash elliptic curve digital signature algorithm.
- Complies with RFC-8032 section 5.2 and FIPS 186-5 standards for robust cryptographic security.
- Supports two types of plaintext:
  - `PlainTextType_Hash64`
  - `PlainTextType_Bytes`
- Requires a signing key of type KeyType_Ed448PrivateKey and a verifying key of type KeyType_Ed448PublicKey.
- Signature size is 114 bytes

Ed448 Mechanism:

- Implements the "pure EdDSA" Ed448 elliptic curve digital signature algorithm.
- Complies to RFC-8032 section 5.2 and FIPS 186-5 standards for cryptographic integrity.
- Signs plaintext of type PlainTextType_Bytes.
- Requires a signing key of type KeyType_Ed448Private for signing and a verifying key of type KeyType_Ed448Public.
- No pre-hashing is performed on the plaintext.
- Signature size is 114 bytes

Remarks:

- Ed448 does not support non-empty context input.
- Ed448 is not accelerated by FPGA.

4.12. RFC5869 HKDF in firmware (NSE-49151)

RFC5869 HKDF has now been added to the 13.5 HSM firmware.

4.13. Attestation of system keys (NSE-49689)

From firmware versions 13.5 onwards the SSH keys used for communication with the HSM are further protected by an internally generated certificate. This certificate binds an SSH key to the ESN of the module which generated the key. Existing warrants validate that the HSM is a genuine Entrust module with that same ESN. The combination of the certificate and warrant provides a way to validate that the SSH keys have not been tampered with after being generated.

The key used for signing system logs is also protected in the same way.

The internal certificates are generated each time the HSM is factory-stated.

If your nShield 5s or nShield 5c has been upgraded from a firmware version earlier than 13.5 you should factory state your HSM to generate the certificates.

4.14. ECC is now enabled by default (NSE-48784)

In firmware versions 13.5 and later, Solo XC and nShield 5s HSMs will report the `EllipticCurve` and `AcceleratedECC` features as permanently enabled.

This will allow the use of ECDSA and ECDH algorithms without the need to first activate these features using the `fet` tool.

The ECCMQV algorithm continues to be licensed as a separate item (Solo XC only).

4.15. Updated nShield 5s Bootloader (NSE-48712)

An updated bootloader for the nShield 5s has been released to fix startup issues encountered with the nShield 5s HSM with some certain servers.

The bootloader is the program that boots the HSM and loads the main application. The nShield 5s has a discrete bootloader that can be updated independently of the Primary and Recovery images. See Upgrade nShield 5s HSM Firmware for more information about how to upgrade to the new v1.4.1 version of bootloader.

4.16. Network status is now exposed via Stattree (NSE-53969)

The Connect and 5c can be configured to provide IP address and status information for their NICs. This information can be viewed with the stattree tool.

4.17. Network interfaces are now monitored on the Connect using SNMP

If enabled, all network interfaces on the Connect are now monitored by SNMP.

4.18. Preload is now ported to Python 3 (NSE-38309)

As previously advised in the v13.3 nShield Security World Release Notes, the `with-nfast` tool and the `--preload` parameter to the `ppmk` tool are obsolete. The `preload` tool is the only tool intended to be used for preloaded sessions. Attempts to call `with-nfast` or `ppmk --preload` will now redirect to the `preload` tool with a warning and may not fully support all previously supported command-line options from those tools. This compatibility forwarding to `preload` may be removed as well in a future release.

4.19. Updated nShield Remote Admin Client (NSE-38313)

The nShield Remote Administration Client has now been updated to run under Python3. The

existing Python2 implementation has been removed from the product.

This new version is available as part of the Security World Software installation only. Security World 13.6.5 does not include an update to the standalone RAC product, which will be updated in a future release. Therefore this updated RAC is available on Windows and Linux only, MacOS support is not provided.

4.20. ACL analyzer for key attestation (NSE-55514)

An ACL analyzer tool has been added to function in combination with the Key Attestation feature.

4.21. NFKM engine now permits asymmetric verification (NSE-39432)

The NFKM engine has been updated to support ECDSA and DSA verification as well as support for RSA verification with PKCS1 and PSS padding modes.

4.22. x931 support for NFKM engine (NSE-39304)

The NFKM engine has been updated to support RSA signing and verification with x931 padding mode.

4.23. nShield PKCS#11 library now supports v3 CKM_SP800_108_COUNTER_KDF (NSE-35939)

CKM_SP800_108_COUNTER_KDF is supported for key derivation with the following restrictions:

- v13.5 or later firmware is required
- The PRF is restricted to SHA-224, SHA-256, SHA-384, SHA-512 or AES CMAC
- The parameters must include no more than two byte arrays, or three if one is a single zero byte.
- `ulWidthInBits` for the counter format and dkm format must be 8, 16 or 32
- Only one key may be derived
- `ulAdditionalDerivedKeys` must be 0

4.24. Support for UNIX domain sockets on Windows (NSE-58561)

The hardserver (nFast Server) service on Windows now uses UNIX domain sockets as the primary local I/O mechanism for communication from client applications when running on Windows 10 or Server 2019 or later, matching the longstanding behaviour on Linux systems.

Clients using nCore from C or Python, or using the CNG or PKCS#11 APIs, use this protocol when it is available. Java clients still use local-loopback TCP exclusively like is the case on Linux.

This change should be transparent to the user, and reduces the time it takes applications to establish a connection to the hardserver at startup, as well as providing a modest improvement in throughput. It also helps avoid conflicts arising from non-nShield applications using the default nShield local-loopback TCP ports 9000 and 9001, provided that Java clients are not required.

Customer applications built using nShield developer libraries from v13.6 will connect using UNIX domain sockets if they are available, but will fallback to local-loopback TCP otherwise, and so can still be run against older nShield Security World installations.

Local client access restrictions are now enforced directly using Windows filesystem DACLs (set on the UNIX domain socket files under `C:\Program Files\nCipher\nfast\sockets`). The configuration of custom access permissions for an alternative Windows Group for unprivileged and privileged connections continues to be possible via the `nt_pipe_users` and `nt_privpipe_users` configuration fields in the `config` file which also continue to be enforced by the hardserver for local-loopback TCP connections.

4.25. CodeSafe changes for Solo XC and Connect XC

Updates have been made to CodeSafe in the XC product (Solo XC and Connect XC). These changes were first introduced in the v13.3.7 release.

4.25.1. CodeSafe fixes in Solo XC Firmware

These fixes require v12.72.3 (FIPS-approved) or v13.5 (latest) Solo XC firmware or v13.6.1 Connect XC netimage containing one of these nShield firmware versions.

4.25.1.1. CodeSafe application MemAllocUser memory reporting

CodeSafe application memory usage via the `MemAllocUser` value in `stattree` was incorrectly

reported in the Solo XC/Connect XC in the following cases:

- Incorrectly reporting 0 when the main thread of the application terminates but there are still background threads running (which is a common idiom in CSEE applications which call `SEElib_StartProcessorThreads()` followed by `ExitThread()` in the main thread)
- Failing to include memory usage of any child processes of the CodeSafe application in the total figure

Both of these issues (Defect NSE-32465) have been corrected.

Memory usage is also now reported based on `VmRSS` (resident set size) rather than `VmSize` (total virtual memory) as that better reflects true physical memory usage of the application. Note that memory usage reporting via `stattree` favors fast reporting, and that if applications need more accurate reporting they can use the `/proc` filesystem to report additional information from within their own application code, e.g. using information from `/proc/self/smaps`.

4.25.1.2. Performance of large commands and replies

There are two nShield firmware issues which affect the performance of processing of large commands and replies that are fixed in this release:

- Defect NSE-35968 caused a 1 second delay in an nCore reply being sent when the reply (total encoded size including overheads) was greater than 8192 bytes. This issue was first fixed in the v13.3 Solo XC firmware but has been backported to v12.72.3 (FIPS-approved). This affects any large reply messages sent to the host-side, including `Cmd_SEEJob` replies from a CodeSafe application.
- Defect NSE-60007 caused some inefficiency in the processing of replies to CodeSafe applications when the CodeSafe application provided a large buffer to receive the reply (as would be the case if the CodeSafe application intended to support the receipt of large replies to core jobs or SEEJobs)

4.25.2. CodeSafe Host-side Fixes

These fixes require v13.6.1 Connect XC netimage or v13.6.5 Security World software version.

4.25.2.1. CodeSafe application handle lifetime fixes

The nShield hardserver service previously implemented a behavior called "SEE Wills" provided by the nCore commands `Cmd_MakeSEEWill` and `Cmd_ExecuteSEEWill` in order to do

shutdown operations for a CodeSafe application.

This behavior was not correct and caused the following issues:

- BSDSEE and GLIBSEE CodeSafe applications started by `see-sock-serv`, `see-stdioe-serv`, and related tools, would not automatically destroy the SEEWorld handle when the client tool exited, requiring the module to be cleared before another CodeSafe application could be started on that module. This was tracked as Defect NSE-34444.
- If a BSDSEE or GLIBSEE application were started remotely on an Connect from a client machine, the Impath resilience (also referred to as parked sessions) feature of the Connect would be disabled for that client session, meaning that any keys loaded by that client would have to be re-loaded if there were a brief network outage. This was tracked as Defect NSE-14926.

"SEE Wills" have been removed, and the normal application handle lifetime behavior is now used for SEEWorld handles, which does not suffer from the above issues. For backwards compatibility with clients from previous versions, the relevant nCore commands continue to be known to the client and Connect hardservers, but they are now no-ops that always return success.

4.25.2.2. Cmd_FastSEEJob fixes

The nShield firmware provides a command `Cmd_SEEJob` for communication between a host machine and a CodeSafe application. This command is always sent by the nShield hardserver as a `LongJob` operation which never times out (unless the module is cleared or fails).

In order to support host-side applications being coded to handle overloaded or hanging operations in a CodeSafe application, the nShield hardserver also provides a wrapper command `Cmd_FastSEEJob` which translates to a `Cmd_SEEJob` sent as a "normal" job that times out after approximately 2 minutes if there is no response received.

This was not implemented correctly and had the following issues (Defect NSE-16280):

- The reply was returned with the command code `Cmd_SEEJob` rather than `Cmd_FastSEEJob` due to incomplete translation. Due to stricter error-checking in client-side library code in v12.50 onwards, this resulted in successful replies from the CodeSafe application sent to jobs that were sent via the `Cmd_FastSEEJob` interface failing with `Status_ServerFailed` in all cases.
- Additionally, `Cmd_FastSEEJob` would be erroneously sent as a `LongJob` when the client system was under load, or if sent from a client to an Connect, meaning that it would not timeout in all cases that it should.

These issues have been fixed, and `Cmd_FastSEEJob` both works functionally in the success case, and also guarantees that it will timeout in all appropriate scenarios. Note that if it times out, the status code returned is `Status_HardwareFailed`. This does not actually mean that the module has failed in this case, nor does it necessarily even mean that the CodeSafe application has irrecoverably failed and it may still be able to respond to subsequent commands.

4.25.2.3. Incorrect check running GLIBSEE application from Connect client

An incorrect check in `see-sock-serv`, `see-stdioe-serv`, and related tools, meant that BSDSEE/GLIBSEE applications run from a client machine against an Connect module would erroneously be refused as failing a feature check. This was tracked as Defect NSE-43686 and the work-around was to pass the `--no-feature-check` parameter when starting the CodeSafe application. This issue has been fixed and the work-around is no longer required.

4.25.3. CodeSafe Developer Software Fixes and Improvements

These fixes are in the v13.6.5 CodeSafe developer software itself. Any CodeSafe library code fixes require the customer application to be rebuilt with the new version of the software to avail of the fix.

4.25.3.1. SEElib commands/replies larger than 8192 bytes

Defect NSE-60631 caused the SEElib library used by Solo XC/Connect XC CSEE applications to fail with a `Status_BufferFull` error when commands and/or replies whose encoded size was over 8192 bytes were sent and/or received. This did not affect all library invocation patterns, but did affect both core jobs (i.e. HSM crypto nCore commands) and `Cmd_SEEJob` command/reply payloads on some paths.

All paths now support the full nCore `MAX_MARSHAL_LEN` encoded size limit (i.e. `262144` bytes) for commands and replies for both core jobs and SEEJobs. Note that the actual payload size (e.g. the size of plaintext or ciphertext in a crypto operation, or the size of buffer in a `Cmd_SEEJob` command or reply) must be somewhat less than the limit in order to allow for encapsulation of command and reply parameters and flags etc.

The new implementation favors performance over memory usage, and so CodeSafe applications using SEElib will use some additional memory as a result of this change.

Applications will achieve the best performance by aiming to batch data transfers, decryption operations, etc. into commands/replies using most of this limit, with a safe margin for overheads, e.g. aiming for 250KB payloads. Note that for best performance, the

v12.72.3 nShield firmware update is needed to address the performance fixes described above for nShield firmware processing of large replies.

4.25.3.2. CodeSafe standard output/error

The following issues relating to the handling of standard I/O have been fixed:

- Defect NSE-15255 : writes to `stderr` in CSEE applications are now correctly written to the trace log, the same as was already the case for writes to stdout
- Defect NSE-51263 : writes to `stdout` in GLIBSEE applications are now written only to host output, and are no longer incorrectly *duplicated* in the trace log. Note that writes to `stderr` in GLIBSEE applications continue to be written only to the trace log.

4.25.3.3. Improved CodeSafe application crash reporting

The crash reporter for CodeSafe applications run on Solo XC/Connect XC has been improved for both CSEE and GLIBSEE applications.

Previously, only minimal reporting was provided for a small number of signals. The reporting is now much more comprehensive, and also includes reporting of extended signal information.

Additionally, a stack trace is reported showing the code which generated the error. Note that for function names to appear in the stack trace (as opposed to just offsets), the CodeSafe application must be built with the `-rdynamic` linker option; that is automatically the case if the application is built with the updated CMake toolchain flags. This adds a separate and much more minimal set of symbols to the executable compared to the symbols produced by `-g`, and unlike `-g` symbols `-rdynamic` dynamic symbols are not removed when an executable is stripped.

All crash reporting appears in the SEE trace log only, which must be enabled and queried in order to retrieve the crash report. If using GLIBSEE, use the `--trace` parameter to `see-sock-serv` and related tools.

4.25.3.4. Improved handling of unavailable syscalls in GLIBSEE applications

When kernel syscalls that are either unsupported or explicitly denied are attempted by CSEE and GLIBSEE applications, the thread in the CodeSafe application making the attempt is stopped. This is usually observed as the application hanging, and makes debugging issues related to syscalls unavailable in the CodeSafe environment difficult.

To assist with this, GLIBSEE applications now contain a syscall compatibility layer which

provides an alternate implementation of library functions which shadows the C library implementation to mitigate some of these issues. This also addresses Defect NSE-57802 where GLIBSEE CodeSafe applications built with v13.x versions of CodeSafe would hang when run on v12.x nShield firmware versions due to a more restricted set of allowed syscalls. GLIBSEE applications built with v13.6.5 CodeSafe support running on v12.x nShield firmware.

The general pattern of behavior of this compatibility layer is as follows:

- When a denied syscall is attempted via its C library wrapper function, `-1` is returned and `errno` is set to `EPERM`
- When an unsupported syscall is attempted via its C library wrapper function, `-1` is returned and `errno` is set to `ENOSYS`
- In some cases, a compatibility implementation of an unavailable syscall's C library wrapper function is provided to enable more library code to work. For example, the `clock_gettime()` nanosecond-precision syscall is denied, but a compatibility implementation that uses the allowed microsecond-precision `gettimeofday()` syscall is now present.
- If a syscall is called "directly" via its syscall number using the variadic `syscall()` function, the above compatibility code is also invoked in a comparable manner, and in cases where a `syscall()` is already allowed it will redirect to the C library `syscall()` implementation to execute as normal.

This compatibility layer is now present in the host-support object files that GLIBSEE applications must be linked with (`${hoststdoe_obj}`, `${hostinetsocks_obj}`, etc.) and so should automatically be included when an application is rebuilt.

It is possible to enable a logging behavior which will cause the attempt to call any denied (`EPERM`) and unsupported (`ENOSYS`) syscalls that are intercepted by the compatibility layer to be logged automatically to the trace log, and optionally to additionally to cause the `SIGSYS` signal to be raised, which by default will cause the crash reporter to report a stack trace in the trace log showing the code which attempted the unavailable syscall. See the new `syscalls.c` example GLIBSEE program which shows how to enable either of these logging modes.

Note that this compatibility layer is not all-encompassing and it is also not included for CSEE as that is not intended as a general-purpose C programming environment. CSEE support and the addition of further compatibility layer functions may be considered if there is customer demand.

4.25.3.5. C++ language support for GLIBSEE

C++11 is now supported for GLIBSEE applications, and the examples now include a `helloplus.cpp` illustrating basic usage of various language and library features from CodeSafe. Note that for C++ exceptions to work correctly in CodeSafe, the shared library version of the compiler runtime libraries (`libgcc` and `libstdc++`) must be used, which is the default (i.e. you must not explicitly statically link against these libraries). The CMake toolchain flags show correct invocation of the compiler and linker for C++ builds.

5. Firmware images

5.1. nShield 5s firmware

The nShield 5s HSM firmware consists of 3 major components:

- Primary Image
- Recovery Image
- Bootloader

This release supplies the different versions of all parts of the HSM firmware required for the different certified configurations. Details on what the components are used for and how to upgrade the different components are detailed in Upgrade nShield 5s HSM Firmware. This includes information about setting the minimum VSN on the nShield 5s. Read this section prior to upgrading any nShield 5s.

The v13.5 firmware is both the latest and Common Criteria certified firmware.

5.1.1. nShield 5s primary firmware

Type	Version	Description	Directory	VSN
FIPS Approved	13.2.4	Updated FIPS firmware released as part of the v13.2 release.	`firmware/nShield5s/fips/nShield5s-13-2-4-vsn4.npkg`	4
FIPS Approved	13.4.5	Re-released v13.4 firmware including CodeSafe 5 support, and various fixes.	`firmware/nShield5s/fips/nShield5s-13-4-5-vsn4.npkg`	4
Latest and **CC Approved**	13.5.1	Latest and Common Criteria Certified firmware with features from v13.5 release.	`firmware/nShield5s/latest/nShield5s-13-5-1-vsn4.npkg`	4

5.1.2. nShield 5s Recovery image

Type	Version	Description	Directory
Latest and **CC Approved**	13.5.0	Latest and Common Criteria Certified nShield5s Recovery image.	`firmware/nShield5s/latest/nShield5s-recovery-13-5-0.npkg`
FIPS Approved	13.2.4	Latest FIPS approved nShield5s Recovery image.	`firmware/nShield5s/fips/nShield5s-recovery-13-2-4.npkg`

5.1.3. nShield 5s Bootloader

This is the first new nShield 5s Bootloader to be officially released. The default version on the nShield 5s as shipped by the factory (v1.1.0) is the FIPS certified version.

Upgrading to this later version is required to operate in a Common Criteria certified configuration. This updated bootloader also addresses startup issues experienced on some servers, as detailed in the Updated nShield 5s Bootloader (NSE-48712).

Type	Version	Description	Directory
Latest and **CC Approved**	1.4.1	Latest and Common Criteria Certified nShield5s Bootloader image.	`firmware/nShield5s/latest/nShield5s-uboot-1-4-1.npkg`

5.2. 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	12.72.3	The latest FIPS approved firmware released as part of the v12.72 release.	`firmware/SoloXC/fips/soloxc-12-72-3-vsn37.nff`	37
Latest	13.5.3	Latest firmware with features from v13.5 release.	`firmware/SoloXC/latest/soloxc-13-5-3-vsn37.nff`	37

5.3. nShield Solo+ firmware

Solo+ firmware has been removed from this release. Please contact nshield.support@entrust.com for the last supported version.

5.4. nShield Edge Firmware

Support for the Edge is still maintained for previous firmware releases.

Type	Version	Description	Directory	VSN
FIPS Approved	12.72.2	The latest FIPS approved firmware released as part of the v12.72 release.	`firmware/Edge/fips/edge-12-72-2-vsn29.nff`	29

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

6. Connect images

The nShield firmware and Connect Image ISO includes v13.6.5 Connect images that contain the Solo XC and nShield 5s firmware described in Firmware images.

6.1. Install a Connect image

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

6.2. nShield 5c images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	13.6.5	13.6 Connect image with FIPS approved firmware	13.4.5	`nethsm-firmware/fips-all-13-6-5-vsn32/`	32
FIPS Legacy	13.6.5	13.6 Connect image with FIPS legacy firmware	13.2.4	`nethsm-firmware/fips-legacy-all-13-6-5-vsn32/`	32
Common Criteria	13.6.5	13.6 Connect image with CC firmware	13.5.1	`nethsm-firmware/cc-all-13-6-5-vsn32/`	32
Latest	13.6.5	13.6 Connect image with latest 13.5 firmware	13.5.1	`nethsm-firmware/latest-all-13-6-5-vsn32/`	32

Both the Common Criteria and Latest nShield 5c images are the same as the latest 5s firmware release is also the Common Criteria certified release.

6.3. Connect XC images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	13.6.5	13.6 Connect image with FIPS firmware	12.72.3	`nethsm-firmware/fips-all-13-6-5-vsn32/`	32
FIPS Legacy	13.6.5	13.6 Connect image with FIPS legacy firmware	12.50.11	`nethsm-firmware/fips-legacy-all-13-6-5-vsn32/`	32
Common Criteria	13.6.5	13.6 Connect image with CC firmware	12.60.15	`nethsm-firmware/cc-all-13-6-5-vsn32/`	32
Latest	13.6.5	13.6 Connect image with latest 13.5 firmware	13.5.3	`nethsm-firmware/latest-all-13-6-5-vsn32/`	32

6.4. Connect+ images

Connect+ images have been removed from this release. Please contact nshield.support@entrust.com for the last supported version.

6.5. Connect CLX images

Connect CLX images have been removed from this release. Please contact nshield.support@entrust.com for the last supported version.

7. Upgrade from previous releases

7.1. Install 13.6.5 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.

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

7.2. Upgrade Solo XC firmware

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

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 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. Please contact nshield.support@entrust.com for any other version of firmware.

Whilst every effort is made to ensure 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.

7.3. Upgrade nShield 5s HSM Firmware

As detailed in the *nShield v13.6.5 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 5s 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 all parts of the HSM firmware and all need to be upgraded to this version to be in a valid certified configuration (both for FIPS and Common Criteria). Details for upgrading the different components are detailed in the following section.

7.3.1. 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
```

As an example, following an upgrade, it should report as follows:

```
"mode": "primary",
"primary-version": "13.5.1-0-3daee55f75",
"recovery-version": "13.5.0-0-e2ec16eefd",
"uboot-version": "1.4.1-0-edb84d6e",
```

7.3.2. 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-13-5-1-vsn4.npkg --esn module-esn
```

and for recovery:

```
hsmadmin upgrade nshield5s-recovery-13-5-1.npkg --esn module-esn
```

7.3.3. Upgrading the nShield 5s Bootloader

The bootloader is the program that boots the HSM and loads the main application. The nShield 5s has a discrete bootloader that can be updated independently of the Primary and Recovery images.

7.3.3.1. Pre-Requisites

Whilst the bootloader is an independent part of the firmware, the capability to upgrade the bootloader on the nShield 5s was introduced as part of the Security World v13.4 firmware release. For earlier versions of firmware prior to v13.4, the nShield 5s firmware must be upgraded to v13.4 as a minimum to enable this bootloader upgrade to work. Contact nShield Support for details of obtaining the v13.4 version of firmware.

7.3.3.2. Upgrading bootloader

Once the primary firmware is at version v13.4 or later, the bootloader can be upgraded using the same hsmadmin upgrade command:

```
hsmadmin upgrade nShield5s-uboot-1-4-1.npkg --esn module-esn
```

Note: Once the bootloader version is upgraded, it is not possible to downgrade the bootloader to the previous version. The Primary and Recovery images can still be downgraded and upgraded independent of this bootloader version.

The v1.4.1 version of bootloader is not FIPS certified and should not be upgraded if a FIPS certified HSM is required.

7.3.4. nShield 5s VSN

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 than 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 *nShield v13.6.5 HSM User Guide*.

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

7.4. Upgrade a Connect XC image

If the 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 Connect image and needs to be first upgraded to an intermediate version. Any of the Connect image versions listed above can be used as an intermediate version. Please contact nshield.support@entrust.com for any other version of Connect image.

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

8.2. 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 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 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**
Oracle Enterprise Linux 8 x64	Y	Y	Y	Y	Y
Oracle Enterprise Linux 9 x64	Y	Y	Y	Y	Y

Security World v13.6.5 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.

8.3. API support

8.3.1. Java

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

Version	Supported
8	Y
11	Y
17	Y
21	Y

8.3.2. Python

This lists the versions of Python that are supported.

Version	Supported
2.7	N
3.11	Y

8.4. Supported hypervisors and 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
VMWare ESXi 8.0	N	Y	N	Y	N

Operating System	Solo+	Solo XC	nShield 5s	Connect+, Connect XC, nShield 5c	Edge
Citrix XenServer 8.2	N	Y	N	Y	N

8.5. Supported compilers for Microsoft Windows C developers

Security World v13.6.5 C libraries for Windows were built using Visual Studio 2022 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 2022.

Version	Supported
2017	N
2022	Y

8.6. Option Pack support

As v13.6 is a Long-Term Supported (LTS) release, the option packs are are being updated to ensure compatability with this release. The table below lists the recommended version of the option pack to use with v13.6. Contact nshield.support@entrust.com for further information about the availability of any option pack.

Option Pack	Compatible Version
Web Services Option Pack (WSOP)	v3.3.1
Time Stamp Option Pack (TSOP)	v8.1.0
Database Security Option Pack (nDSOP)	v2.1
Cloud Integration Option Pack (CIOP)	v2.2.3
nShield Container Option Pack (nCOP)	v1.1.2

9. Documentation updates

To reduce duplication and improve clarity and accessibility of information, Entrust are restructuring and updating elements of the nShield product documentation during 2024. Security World 13.6.5 introduces some of these changes to the documentation as detailed below.

Read the relevant parts of each guide before and while using your nShield HSMs.

Previous Documents	New Documents	Changes
nShield Security Manual	nShield Security Manual	No changes, continues to provide advice on the secure operation of the product.
nShield Connect Install Guide nShield 5c Install Guide nShield Edge Install Guide nShield Solo and Solo XC Install Guide nShield 5s Install Guide	nShield Hardware Install and Setup Guides	Install guide information for all supported nShield HSMs is now in a single guide. This guide explains how to physically install and get started with your nShield HSMs.
	Security World Software Installation Guide	This guide explains how to install, upgrade, and uninstall the Security World software.
nShield Connect User Guide nShield 5c User Guide nShield Edge User Guide nShield Solo User Guide nShield 5s User Guide	nShield HSM User Guide	This guide contains hardware and firmware information specific to each type of nShield HSM, as well as guidance on managing nShield HSMs in general.
	nShield Security World Management Guide	This guide contains information about creating and managing Security Worlds.
	nShield Utilities	This guide provides information on the utilities provided as part of the Security World installation.
	nShield Security World Key Management Guide	This guide explains how to use Security World to perform Key Management.

Documentation is also provided for the major APIs into nShield, whose structure has not changed. This includes:

- nCore API Guide
- Microsoft Crypto API Guide

- Microsoft CNG API Guide
- nCipher KM JCA JCE CSP API Guide
- PKCS11 API Guide

The nToken Installation 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.

10. Known and fixed issues

Reference	Scope	Status	Description
NSE-66415		Open	The appliance-cli gethsmstatus command returns a 'Failed to retrieve status' error when executed against Legacy FIPS Connect image. This means the version information for the Legacy FIPS Connect image cannot be retrieved at this time. **Issue first found** in 13.6
NSE-65799		Open	A stack trace will be displayed on SLES12, this is a regression but does not affect the Security World software installation. **Issue first found** in 13.6
NSE-64700	Client-side	Resolved	Fixed issue where an error reported by nethsmadmin for an incorrect URL was wrong. **Resolved** in 13.6.5 client-side.
NSE-64070	Client-side	Resolved	Made the audit logging service more user friendly for certain conditions. **Resolved** in 13.6.5 client-side.
NSE-63880	Connect (5c & XC)	Resolved	Fixed issue where the KeySafe 5 Agent could object leak during CodeSafe 5 updates. **Resolved** in 13.6.5 Connect Images.
NSE-63870	Client-side	Resolved	Fixed issue where nfdiag stated an incorrect error on successful completion. **Resolved** in 13.6.5 client-side.
NSE-63848	Connect (5c & XC) and Client-side	Resolved	Fixed an issue where the server-side log message regarding license limits was misleading. **Resolved** in 13.6.5 client-side and 13.6.5 Connect Images.

Reference	Scope	Status	Description
NSE-63635	Client-side	Resolved	Fixed a performance issue identified during soak testing. **Resolved** in 13.6.5 client-side.
NSE-63502		Open	When using KeySafe5 with the agent on the Connect the following error will populate the logs 'Command failed: monitor codesafestats get-all'. Users should increase the codesafe_update_interval using the ks5agent command via the Connect CLI. ks5agent cfg codesafe_update_interval=48h If you wish the logs to be cleared then enabling the Audit tooling will expire the system logs containing the above error. **Issue first found** in 13.6
NSE-63449	Client-side	Resolved	Fixed an issue with PKCS11 key generation certificates. **Resolved** in 13.6.5 client-side.
NSE-63444	Client-side	Resolved	Fixed an issue with PKCS11 key type enums. **Resolved** in 13.6.5 client-side.
NSE-63387	Client-side	Resolved	Fixed a PKCS11 encoding issue when using Edwards CKA_EC_POINT. **Resolved** in 13.6.5 client-side.
NSE-63316	Connect (5c only)	Resolved	Fixed issue hsmdiagnose utility on the nShield 5c Connect CLI did not work at all. **Resolved** in 13.6.5 5c Connect Images.

Reference	Scope	Status	Description
NSE-63086	Connect (5c & XC)	Resolved	Fixed issue where the Connect FPUI 'Factory state' warning text was truncated. **Resolved** in 13.6.5 Connect Images.
NSE-62788	Connect (5c & XC)	Resolved	Fixed an issue where the diff utility was missing on the Connect **Resolved** in 13.6.1 Connect image.
NSE-62705	Connect (5c & XC)	Resolved	Fixed issue with Connect ping screen (1-1-1-7-1) was missing information. **Resolved** in 13.6.5 Connect Images.
NSE-62604	Connect (5c & XC)	Resolved	Fixed issue where the cosmod process on the Connect would report as not running. **Resolved** in 13.6.5 Connect Images.
NSE-61967		Open	Codesafe 5's tar command will currently be killed by the seccomp. Currently users should avoid calling this command until this issue is resolved. **Issue first found** in 13.4
NSE-61694	Client-side	Resolved	Fixed a PKCS11 issue where corruption could occur with certain library calls. **Resolved** in 13.6.5 client-side.
NSE-61181	Connect (5c & XC)	Resolved	Fixed an issue where there as missing stderr logging from config-update on Connect **Resolved** in 13.6.1 Connect image.
NSE-61002	Firmware (5s only)	Resolved	Fixed an issue where the Audit Init Log continuously grows **Resolved** in 13.5.1 firmware.

Reference	Scope	Status	Description
NSE-60958	Client-side	Resolved	Fixed and issue where a SEH exception occurred in CNG Provider's NCryptEncrypt/NCryptDecrypt **Resolved** in 13.6.3 client-side.
NSE-60956	Client-side	Resolved	Fixed an issue with HSM Pool mode where nShield Connects that were once usable but became no longer usable by a client machine (no longer in the Security World, or the updated `module_ESN` file was not copied across to that client machine after re-loading the World on that Connect before going operational again) could cause the whole HSM Pool to be unusable resulting in application failure. The fix requires an updated SecWorld installation on the client, but does not require an update to the nShield Connect itself. **Resolved** in 13.6.3 client-side.
NSE-60746	Client-side	Resolved	cknfkmid now recognises the AES key type **Resolved** in 13.6.3 client-side.
NSE-60631	Client-side & Firmware (Solo XC only)	Resolved	Fixed an issue where the SEELib library for SoloXC did not support commands and replies over 8K (for both core jobs and SEEJobs) in some execution modes. **Resolved** in 13.6.3 client-side and 13.5.3 firmware.
NSE-60554		Open	TUAK and Milenage session key generation performance has decreased due to the need to generate key generation certificates at the point of key generation. **Issue first found** in 13.4
NSE-60363	Connect (5c & XC)	Resolved	Fixed issue where the Connect logs pushed via syslog contained 'killing children'. **Resolved** in 13.6.5 Connect Images.

Reference	Scope	Status	Description
NSE-60232	Client-side	Resolved	Fixed and issue where Java garbage collection could delete preloaded keys from the module. **Resolved** in 13.6.3 client-side.
NSE-59952	Firmware (5s only)	Resolved	Fixed an issue where the binaries contain full function/object symbol names. **Resolved** in 13.5.1 firmware.
NSE-59848	Client-side	Resolved	Fixed an issue with nfpython bitmap equality. **Resolved** in 13.6.3 client-side.
NSE-59633	Connect (5c & XC)	Resolved	Fixed issue where a benign warning message was displayed in the Connect syslog. **Resolved** in 13.6.5 Connect Images.
NSE-59627	Connect (5c & XC)	Resolved	Various CVE resolutions. **Resolved** in 13.6.1 Connect image.
NSE-59574	Firmware (5s only)	Resolved	Fixed an issue where invalid SSH tunnel keys could be set via csadmin. **Resolved** in 13.5.1 firmware.
NSE-59572	Firmware (Solo XC only)	Resolved	Fixed an SOS OLC when doing decryption. **Resolved** in 13.5.3 firmware.
NSE-59481	Documentation	Resolved	Fixed an issue where configuration information for Codesafe 5 was missing from the user documentation. **Resolved** in 13.6.3 documentation.

Reference	Scope	Status	Description
NSE-59466	Client-side	Resolved	Fixed issue where CyberJack Base Components would occasionally fail to uninstall on Windows systems. **Resolved** in 13.6.5 client-side.
NSE-59422	Client-side	Resolved	Fixed an issue where PKCS#11 would core dump changing public key permissions when not logged in. **Resolved** in 13.6.3 client-side.
NSE-59417	Client-side	Resolved	Fixed an issue where Codesafe examples would trigger a MemAllocUser error. **Resolved** in 13.6.3 client-side.
NSE-59399	Firmware (5s only)	Resolved	Fixed an issue with error not being displayed if loading bad firmware onto HSM. **Resolved** in 13.5.1 firmware.
NSE-59249	Firmware (5s only)	Resolved	Fixed an issue where erroneous smartcard messages were written to the system log. **Resolved** in 13.5.1 firmware.
NSE-58953	Firmware (5s only)	Resolved	Fixed incorrect timing issue. **Resolved** in 13.5.1 firmware.
NSE-58882	Client-side	Resolved	Fixed an issue with C_FindObjects not always finding new objects. **Resolved** in 13.6.3 client-side.
NSE-58765	Connect (5c & XC)	Resolved	Fixed an issue where multiple clients could be attached to the same remote session at the same time. **Resolved** in 13.6.1 Connect image.

Reference	Scope	Status	Description
NSE-58706	Client-side	Resolved	Fixed an issue where VPN tools could break hardserver connections. **Resolved** in 13.6.3 client-side.
NSE-58270	Client-side	Resolved	Fixed an issue where our JCE implementation silently ignores AlgorithmParameters for RSA-OAEP. **Resolved** in 13.6.3 client-side.
NSE-58090	Firmware (Solo XC only)	Resolved	Fixed an issue where performance shaping could cause excessive delays. **Resolved** in 13.5.3 firmware.
NSE-57802	Client-side	Resolved	Fixed an issue where SEE machine glibc stdoe examples could freeze with 12.X firmware. **Resolved** in 13.6.3 client-side.
NSE-57727	Client-side	Resolved	Fixed an issue where PKCS#11 did not check for absent parameters in OAEP keywrap. **Resolved** in 13.6.3 client-side.
NSE-57619	Client-side	Resolved	Fixed an issue where the incorrect error was returned if FIPS auth token was not in the cardlist. **Resolved** in 13.6.3 client-side.
NSE-57404	Connect (5c & XC)	Resolved	Fixed a regression from a previous bugfix. **Resolved** in 13.6.1 Connect image.
NSE-57267	Client-side	Resolved	Fixed an issue with SNMP mibs not containing serial number of offending module when hardware events are triggered. **Resolved** in 13.6.3 client-side.

Reference	Scope	Status	Description
NSE-57173	Client-side	Resolved	Fixed an issue where hsmadmin reset would fail if the HSM provided an invalid ESN. **Resolved** in 13.6.3 client-side.
NSE-57141	Client-side	Resolved	Fixed an issue where the FormatToken command can leave the device locked when handling errors. **Resolved** in 13.6.3 client-side.
NSE-57123	Client-side	Resolved	Fixed an issue with nCipherKM JCE debug missing debugFuncEnd causing unreadable logs. **Resolved** in 13.6.3 client-side.
NSE-57120	Client-side	Resolved	Fixed an issue with Solo XC driver being incompatible with Kernel version 6.4. **Resolved** in 13.6.3 client-side.
NSE-57013	Client-side	Resolved	Fixed an issue where nfp driver prints log entries across 3 lines instead of 1. **Resolved** in 13.6.3 client-side.
NSE-56991	Client-side	Resolved	Fixed an issue where DSACommVariableSeed occasionally fails. **Resolved** in 13.6.3 client-side.
NSE-56895	Client-side	Resolved	Fixed an issue where PKCS#11 Derive failure results in leaked template object. **Resolved** in 13.6.3 client-side.
NSE-56619	Client-side	Resolved	Fixed an issue where the hardserver could terminate in some error states. **Resolved** in 13.6.3 client-side.

Reference	Scope	Status	Description
NSE-56604	Client-side	Resolved	Fixed an issue where the priority queueing configuration in the [module_settings] of the config file were not always respected. Note that it is not generally recommended to use these settings, as usually best throughput is achieved with the default scheduling. **Resolved** in 13.6.3 client-side.
NSE-56579	Client-side	Resolved	Fixed an issue where starting hardserver connections could be delayed when modules are failed or under load, and errors about GenerateRandom failing could appear in logs. **Resolved** in 13.6.3 client-side.
NSE-56549	Client-side	Resolved	Fixed an issue where hsmadmin logs get command shows incorrect options on production modules. **Resolved** in 13.6.3 client-side.
NSE-56505	Connect (5c & XC)	Resolved	Fixed issue where it was not possible to setup the RFS via the FPUI if interface #2 is configured with uncontactable IP. **Resolved** in 13.6.5 Connect Images.
NSE-56457	Firmware (Solo XC only)	Resolved	Fixed an issue with performance throttling. **Resolved** in 13.5.3 firmware.
NSE-56354	Connect (5c & XC)	Resolved	Fixed an issue with CLI tab completion logging out of an active session. **Resolved** in 13.6.1 Connect image.
NSE-55780		Open	Starting a CodeSafe 5 SEE machine on an nShield 5c mentions "Could not find nshield network interfaces for service discovery" in the verbose output. **Issue first found** in 13.4

Reference	Scope	Status	Description
NSE-55595	Client-side	Resolved	Fixed an issue where NFAST_BIN needed to be in the PATH variable for migrate-world to operate. **Resolved** in 13.6.3 client-side.
NSE-55594	Client-side	Resolved	Fixed an issue where the "make clean" command failed to clean driver files. **Resolved** in 13.6.3 client-side.
NSE-55428		Open	Building classic Codesafe examples fails with older compiler. **Issue first found** in 13.4
NSE-55378		Open	Minor inconsistency when enabling autostart via csadmin config. **Issue first found** in 13.4
NSE-55367	Client-side	Resolved	Fixed an issue with unhelpful message from hsmadmin with no returned results. **Resolved** in 13.6.3 client-side.
NSE-55341	Client-side	Resolved	Fixed an issue where a non-human readable error when a random certificate is attempted to be added via csadmin ids add. **Resolved** in 13.6.3 client-side.
NSE-55142		Open	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. **Issue first found** 13.4
NSE-55034	Connect (5c & XC)	Resolved	Fixed issue where IPv6 SLAAC would only work on 1 interface at a time. **Resolved** in 13.6.5 Connect Images.

Reference	Scope	Status	Description
NSE-54793	Client-side	Resolved	Fixed issue where migrate-world would fail if OCS had a timeout set. **Resolved** in 13.6.5 client-side.
NSE-54569	Client-side	Resolved	Fixed an issue where if NFAST_KEYPROT_PASS is in place hsmdiagnose asks for Updater password twice. **Resolved** in 13.6.3 client-side.
NSE-54365	Client-side	Resolved	Fixed an issue with threading with SEE applications. **Resolved** in 13.6.3 client-side.
NSE-54338	Client-side	Resolved	Removed obsolete executables installed in the /opt/nfast/bin/ directory. **Resolved** in 13.6.3 client-side.
NSE-54312	Connect (5c & XC)	Resolved	Disable various peripheral devices on Connect when in different modes. **Resolved** in 13.6.1 Connect image.
NSE-53588	Client-side	Resolved	Fixed various CVEs in Open Source Software. **Resolved** in 13.6.3 client-side.
NSE-53574	Client-side	Resolved	Fixed an issue where PKCS#11 key generation fails if CKNFAST_RELOAD_KEYS is set when token is no preloaded. **Resolved** in 13.6.3 client-side.
NSE-53441	Client-side	Resolved	Fixed an issue with postload-bsdlib permissions **Resolved** in 13.6.3 client-side.

Reference	Scope	Status	Description
NSE-53307 NSE-58846	Connect (5c & XC)	Resolved	Improved the handling of internal log files on the connect particularly in the presence of high log traffic and fix of logrotate errors. **Resolved** in 13.6.1 Connect image.
NSE-53108	Connect (5c & XC)	Resolved	Fixed an issue Connect fans running at full speed. **Resolved** in 13.6.1 Connect image.
NSE-52862	Client-side	Resolved	Fixed a typo in hsc_configureslots. **Resolved** in 13.6.3 client-side.
NSE-52785	Client-side	Resolved	Fixed error handling for nfkm_getinfox. **Resolved** in 13.6.3 client-side.
NSE-52775	Client-side	Resolved	Fixed an issue with DecryptMarshaled missing restrictions when in FIPS. **Resolved** in 13.6.3 client-side.
NSE-52303	Client-side	Resolved	Changed to use monotonic clock for certain timers in the hardserver. **Resolved** in 13.6.3 client-side.
NSE-52177	Client-side	Resolved	ASN.1 decoders should now no longer ignore trailing bytes. **Resolved** in 13.6.3 client-side.
NSE-51263	Client-side	Resolved	Fixed an issue where GLIBSEE would duplicate stdout in trace log. **Resolved** in 13.6.3 client-side.

Reference	Scope	Status	Description
NSE-50965	Client-side	Resolved	Fixed issue where the hardserver would mistakenly recycle key ids. **Resolved** in 13.6.5 client-side.
NSE-50692	Client-side	Resolved	Fixed an issue where the `nFast Server` (hardserver) service could fail to restart correctly or fail to find the nShield 5s module when running `hsmadmin enroll` on Windows. **Resolved** in 13.6.3 client-side.
NSE-50309	Client-side	Resolved	Make "hsmadmin enroll" error messages clearer. **Resolved** in 13.6.3 client-side.
NSE-50284	Connect (5c & XC)	Resolved	Fixed an issue relating to the transfer of femcerts to Connect failing when loading a Restricted SEE machine. **Resolved** in 13.6.1 Connect image.
NSE-50021	Client-side	Resolved	Fixed an issue where the hardserver attempted to load HSM-protected KNETI keys in module modes where that was not supported, resulting in Nonfatal errors in the hardserver log. **Resolved** in 13.6.3 client-side.
NSE-49372	Client-side	Resolved	Tidied up -h option for various shipped utilities. **Resolved** in 13.6.3 client-side.
NSE-49032	Client-side	Resolved	Updated Reiner TVD drivers. **Resolved** in 13.6.3 client-side.

Reference	Scope	Status	Description
NSE-48990	Documentation	Resolved	Made documentation around prime generation clearer. **Resolved** in 13.6.3 documentation.
NSE-48428	Connect (5c & XC)	Resolved	Connect feature files are no longer copied using the "3-2-2 Load Security World" / "3-3-1 Update World files" menu options in the Connect front panel. This is because the feature files were not generally applied in this context, but could accidentally result in overwriting a newer client license with an older more restricted one. Features should be applied either using one of the "2-3 HSM feature enable" menu options or using the "nethsmadmin --apply-feature" remote option. **Resolved** in 13.6.1 Connect image.
NSE-48073		Open	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. **Issue first found** in 13.3
NSE-46704	Client-side	Resolved	Fixed an issue where PKCS#11 ECDH1 could not produce HMAC keys. **Resolved** in 13.6.3 client-side.
NSE-46680	Client-side	Resolved	Fixed an empty public blob in key file when using Python3 recordkey. **Resolved** in 13.6.3 client-side.
NSE-46612	Firmware (5s only)	Resolved	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. **Resolved** in 13.5.1 firmware.

Reference	Scope	Status	Description
NSE-46511	Client-side	Resolved	Various CVE remediations in Open Source Software. **Resolved** in 13.6.3 client-side.
NSE-46497	Client-side	Resolved	Fixed an issue where generatekey did not reject invalid key idents. **Resolved** in 13.6.3 client-side.
NSE-43686	Connect (5c & XC)	Resolved	Fixed an issue where glibsee/bsdlib CodeSafe applications could not be run from a remote client via see-sock-serv / see-stdioe-serv, and related utilities, unless the --no-feature-check parameter was passed. The --no-feature-check parameter is no longer necessary. A Security World client-side software update is required to get this fix. No Connect update is required. **Resolved** in 13.6.1 Connect image.
NSE-42314	Client-side	Resolved	Fixed an issue where CNG forbade ECDSA with small hashes in FIPS mode. **Resolved** in 13.6.3 client-side.
NSE-42127	Client-side	Resolved	Fixed an issue where nfkmverify does not work with foreign KMWK. **Resolved** in 13.6.3 client-side.
NSE-41730	Client-side	Resolved	Fixed an issue where an extraneous but harmless error message was reported in the hardserver log if an address for audit syslog was not configured in config. **Resolved** in 13.6.3 client-side.
NSE-41465	Client-side	Resolved	Fixed an issue where new-world would create worlds with unusable ACS cards. **Resolved** in 13.6.3 client-side.

Reference	Scope	Status	Description
NSE-39842	Client-side	Resolved	Fixed an issue where higher debug levels could cause PKCS#11 to return incorrect attribute lengths. **Resolved** in 13.6.3 client-side.
NSE-39767	Documentation	Resolved	Fixed a documentation issue where Mech_ECDHKeyExchange keytypes were incorrect. **Resolved** in 13.6.3 documentation.
NSE-39453	Client-side & Firmware (Solo XC only)	Resolved	Fixed an SOS OLC crash that could occur whilst a Solo XC's SEE machine handled multiple connections. **Resolved** in 13.6.3 client-side and 13.5.3 firmware.
NSE-39448	Client-side	Resolved	Fixed misreporting of performance for CNG during soak testing. **Resolved** in 13.6.3 client-side.
NSE-39031		Open	In Security World v12.10 a compliance mode was added to the Connect to allow compliance with USGv6 or IPv6 Ready requirements. **Issue first found** in 12.80
NSE-38552	Client-side	Resolved	Fixed issue with CNG and CAPI providers doing DLL cleanup at the wrong time. **Resolved** in 13.6.5 client-side.
NSE-35501	Client-side	Resolved	Fixed a buffer overflow issue with ASAN for some compiled example code. **Resolved** in 13.6.3 client-side.
NSE-35295	Client-side	Resolved	Remove duplicated WxPython module. **Resolved** in 13.6.3 client-side.

Reference	Scope	Status	Description
NSE-34444	Client-side	Resolved	Fixed an issue where the module had to be cleared after running a glibsee/bsdlib CodeSafe application in order to be able to run or re-run a CodeSafe application again. This issue is resolved by updating the Security World client-side software. A firmware or Connect netimage update is not required. **Resolved** in 13.6.3 client-side.
NSE-33812	Client-side	Resolved	Removed redundant app types from generatekey. **Resolved** in 13.6.3 client-side.
NSE-33636	Client-side	Resolved	Windows hardserver (nFast Server service) no longer fails startup if the default local-loopback TCP ports (9000/9001) are in use by another application provided that the Windows OS version supports UNIX domain sockets (Server 2019/Windows 10 and later) and TCP ports haven't been explicitly enabled in config. **Resolved** in 13.6.3 client-side.
NSE-32465	Client-side	Resolved	Fixed issues with reporting of CodeSafe application memory usage in MemAllocUser stattree value in Solo XC and Connect XC: * Incorrectly reporting 0 when the main thread of the application terminates but there are still background threads running (which is a common idiom in applications using SEElib_StartProcessorThreads) * Failing to include memory usage of any child processes of the CodeSafe application Memory usage is also now reported based on VmRSS (resident set size) rather than VmSize (total virtual memory) as that better reflects true physical memory usage of the application. Note that memory usage reporting via stattree favours fast reporting, and that if applications need more accurate reporting they can use the /proc filesystem to report additional information from within their own application code, e.g. using information from /proc/self/smaps. **Resolved** in 13.6.3 client-side.
NSE-32229	Client-side	Resolved	Fixed a defect where Ed25519 operations with long inputs could fail. **Resolved** in 13.6.3 client-side.

Reference	Scope	Status	Description
NSE-32101	Client-side	Resolved	Fixed an nShield Remote Administration Client issue where making a new dynamic slot association after pressing "Back" from the end of the wizard would fail with a card exclusive lock error. **Resolved** in 13.6.3 client-side.
NSE-31522	Client-side	Resolved	Fixed an issue that caused preload -H to fail with dynamic slots until they were mapped. **Resolved** in 13.6.3 client-side.
NSE-28606		Open	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.
NSE-25860	Client-side	Resolved	Fixed up new-world -c command line option error message for unrecognized cipher-suite. **Resolved** in 13.6.3 client-side.
NSE-25619	Client-side	Resolved	Corrected spelling error during client license upgrade. **Resolved** in 13.6.3 client-side.
NSE-25401		Open	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. **Issue first found** in 12.60
NSE-25385	Connect (5c & XC)	Resolved	Alter Connect firewall rules. **Resolved** in 13.6.1 Connect image.

Reference	Scope	Status	Description
NSE-24335		Open	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 **Issue first found** in 12.50
NSE-23982		Open	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. **Issue first found** in 12.50
NSE-22323	Client-side	Resolved	Fixed issue where `--pool` option output from `enquiry --help` and `nfkminfo --help` did not match User Guide. **Resolved** in 13.6.3 client-side.
NSE-20147	Client-side	Resolved	Fixed issue where KCDSA key generation would not adequately check parameters. **Resolved** in 13.5.1 amd 13.5.3 firmware.
NSE-19732	Client-side	Resolved	CodeSafe toolchain definitions that allow GLIBSEE SEE machines to be written in C are now provided, along with an example that shows using C language and library features from C. Note that dynamic (not static) linking against the C and C runtimes is required (which is the default). **Resolved** in 13.6.3 client-side.

Reference	Scope	Status	Description
NSE-16280	Client-side	Resolved	Fixed issues where CodeSafe SEE Jobs sent via the Cmd_FastSEEJob command were not processed correctly: (1) they now work functionally in systems that have an updated Security World software (this is not a SEElib issue) (2) they are now guaranteed to timeout if the CodeSafe application does not reply in all cases (use Cmd_SEEJob if the SEE Job should never timeout) provided that Security World is updated and also the netimage if the jobs are being sent by a remote client to an Connect. **Resolved** in 13.6.3 client-side.
NSE-15255	Client-side	Resolved	Fixed an issue where stderr from CodeSafe CSEE applications was not written to the trace log. Now messages written to both stdout and stderr are written to the trace log. CodeSafe applications must be built against the updated libraries in order to benefit from the fix. **Resolved** in 13.6.3 client-side.
NSE-14926	Connect (5c & XC)	Resolved	Fixed an issue where Connect Impath session resilience did not work if the remote client ran a CodeSafe glibsee/bsdlib application via see-sock-serv/see-stdioe-serv and related utilities. Updating either the Security World software on the client, the netimage of the Connect, or both, resolves the issue. **Resolved** in 13.6.3 client-side and 13.6.1 Connect image.
NSE-14406		Open	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. **Issue first found** in 12.50
NSE-14166	Client-side	Resolved	Fixed a crash in the cngimport tool that could occur when its passphrase dialog window was left active for several minutes. **Resolved** in 13.6.3 client-side.
NSE-11473	Client-side & Firmware	Resolved	Fixed an issue where ACL reduction was too strict for non-volatile and host use limits. **Resolved** in 13.6.3 client-side, 13.5.1 and 13.5.3 firmware.

Reference	Scope	Status	Description
NSE-10000	Connect (5c & XC)	Resolved	Fixed issue where creating an ACS/OCS with no passphrase can result in one being set. **Resolved** in 13.6.1 Connect image.
NSE-9583	Client-side	Resolved	Fixed an issue where HSM-protected KNETI files were not regenerated after they became invalidated due to initunit or world creation/loading, resulting in UnknownKM errors in hardserver log. To repair the situation with any stale KNETI files from before this fix, delete the kneti-ESN files under the hardserver.d directory (root or administrators' access will be required) and then clear the module or restart the hardserver. Any stale files will also be automatically replaced next time initunit or world creation/loading occurs. **Resolved** in 13.6.3 client-side.
NSE-3946	Client-side	Resolved	Fixed an issue where clients of Connects could fail to automatically recover from errors if they occurred at certain points in the client setup sequence. This usually appeared with the symptom of InvalidState appearing in enquiry for the connection status for that module. Connections are now retried for such errors in the same way as was the case for network failures. **Resolved** in 13.6.3 client-side.
NSE-3503	Client-side	Resolved	Fixed issue where rfs-sync could fail if Cmd_GenerateRandom was unavailable. **Resolved** in 13.6.3 client-side.
NSE-716	Client-side	Resolved	Fixed an issue where KeyType_DSAPrivate nCore API was misleading. **Resolved** in 13.6.3 client-side.
NSE-10	Client-side	Resolved	Fixed issue where KCDSA key generation would not adequately check parameters. **Resolved** in 13.6.3 client-side.