nShield Security World

nShield Security World v13.7.3 Release Notes

14 July 2025

Table of Contents

1. Introduction

These release notes apply to the release of version 13.7.3 of Security World 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 v13.7

Security World version v13.7 introduces new features and enhancements as described in Features of Security World v13.7. It also corrects a number of defects that have been identified in earlier releases.

Security World 13.7.3 is a **Standard-Term Supported (STS)** release. This release is designed to give early access to new nShield features and has a shorter support period.
For long-term support (LTS), frequent stability updates and certified firmware, it is recommended to use the v13.6 Long-Term Support release. See the nShield Security World Release Information for details of the supported versions and the STS & LTS policy.

This release contains updates to the following products:

- Updated firmware for nShield 5s and Solo XC
- Updated Connect images for nShield 5c and Connect XC
- Updated Linux and Windows Security World and Codesafe ISOs

CodeSafe 5 libraries, configuration and wire formats have changed in this release. See Codesafe 5 Automatic Configuration for details.

If a preview release of Security World v13.7 is currently installed on your system be sure to update the client-side on your system. The Solo XC and nShield 5s firmware, as well as the Connect XC and Connect 5c images have not changed since the preview release and do not need to be updated.

1.3. Versions of these Release Notes

Revision	Date	Description
1.7	2025-07-14	*Security Manual* updated to clarify • The difference between erasing a security world and factory stating the HSM • The FIPS-certification scope and tamper resistance boundary for the Connect XC and 5c • The limitations of the tamper log • User roles and authentication configuration
1.6	2025-06-02	Java support updated in the user documentation, it was already correct in these release notes.
1.5	2025-05-30	Firewall recommendations updated in the *Security Manual* (HSM behind dedicated firewall).
1.4	2025-04-11	KeySafe is no longer supported in v13.7 and later Security World Software. See Deprecated and discontinued features.
1.3	2025-04-08	Release notes for the release of v13.7.3.
1.2	2025-04-07	Release notes for the release of v13.7.3.
1.1	2025-03-07	Release notes for the preview release of v13.7.2. These release notes are preview notes and will be updated over time. They may not contain full details of all the changes in the v13.7 release.

Revision	Date	Description
1.0	2025-02-07	Release notes for the preview release of v13.7.1. These release notes are preview notes and will be updated over time. They may not contain full details of all the changes in the v13.7 release.

2. Product versions

2.1. Security World software versions

Version	Date	Description
v13.7.3	2025-04-04	Full Release of the 13.7.3 Linux and Windows ISOs.
v13.7.2	2025-03-07	Preview release of the 13.7.2 Linux ISO.

2.2. CodeSafe Developer software versions

Version	Date	Description
v13.7.3	2025-04-04	Full Release of the 13.7.3 SecWorld and Codesafe Linux and Windows ISOs.
v13.7.2	2025-03-07	Preview release of the 13.7.2 SecWorld and Codesafe Linux ISOs.

2.3. Firmware and Connect ISO versions

Version	Date	Description
v13.7.3	2025-04-04	Full Release of the 13.7.3 FW ISO including the updated 13.7 Connect images and firmware.
v13.7.1	2025-02-07	Preview release of the 13.7.1 FW ISO including the updated 13.7 Connect images and firmware.

2.4. nShield Firmware versions

Version	Date	Description
v13.7.1	2025-04-04	Full Release of 13.7 Firmware for nShield 5s and nShield Solo XC HSMs containing the latest features and fixes.
v13.7.1	2025-02-07	Preview release of 13.7 Firmware for nShield 5s and nShield Solo XC HSMs containing the latest features and fixes.

2.5. Connect image versions

Version	Date	Description
v13.7.1	2025-04-04	Full Release of 13.7 images for nShield 5c and nShield Connect XC HSMs containing the latest features and fixes.
v13.7.1	2025-02-07	Preview release of 13.7 images for nShield 5c and nShield Connect XC HSMs containing the latest features and fixes.

3. Features of Security World v13.7

3.1. New v13.7.1 Connect Images

Refer to Connect images for more information on the new v13.7.1 Connect images.

Refer to Known and fixed issues for more information on fixed issues in the new v13.7.1 Connect images.

3.1.1. Unset module RTC upgrade issue on Connect 5c units

Connect 5c only Due to NSE-69020 if the Connect 5c unit is using a v13.6+ image and the RTC is not set it will result in an upgrade failure.

The following **Connect 5c** images are impacted by NSE-69020:

Release	Connect 5c Version
Security World v13.6.3 LTS Release	v13.6.1
Security World v13.6.5 LTS Update 1	v13.6.4
Security World v13.6.8 LTS Update 2	v13.6.7
Security World v13.7.3 STS Release 1	v13.7.1

To determine if your **Connect 5c** unit has the RTC set correctly, execute the `ncdate` command against the target Connect 5c unit.

A Connect 5c with the correct RTC date and time set should display a variance of the following:

```
# ncdate -m1
Local time is 07:03:54.943 2025.03.12
```

A Connect 5c with the the incorrect RTC date and time set will display a variance of the following:

```
# ncdate -m1
Local time is 07:03:54.943 1970.03.12
```

Please contact nshield.support@entrust.com if the RTC for your **Connect 5c** unit is incorrectly set for more assistance.

3.2. Codesafe 5 Firmware and SDK improvements (NSE-66633)

Security World v13.7 introduces firmware and SDK improvements for Codesafe 5.

These improvements include:

- Codesafe 5 automatic configuration, refer to Codesafe 5 Automatic Configuration for more information
- Automatic startup of the `hsc_codesafe` utility, refer to Automatic Startup for more infor mationfor more information
- Startup configuration debugging, refer to Debugging startup configuration for more information
- Connection status monitoring, refer to Monitoring Connection Status for more informa tion
- Revised set of CodeSafe 5 system calls, refer to Revised set of CodeSafe 5 system calls for more information
- Support for additional signatures on CodeSafe 5 images, refer to Support for additional signatures on CodeSafe 5 images for more information
- Support for remote configuration of CodeSafe 5 on the nShield 5c, refer to Support for remote configuration of CodeSafe 5 on the nShield 5c for more information

3.2.1. Codesafe 5 Automatic Configuration

- A new `[codesafe]` configuration section has been added to the client-side `config` file which supports automatic loading, configuration and running of CodeSafe 5 applica-tions
- A configuration-helper program `hsc_codesafe` is run automatically by the `hardserver` during module startup (or after module clear) to process this configuration, with SEE-Jobs now supported via the `hardserver` again via a mutually authenticated SSH tunnel.
- The internal `ncssh` tool has been updated to support setting up the SSH tunnels auto-matically (external tools such as OpenSSH are no longer required) and is run automati-cally by this configuration-helper.
- Privileged clients of nShield 5c are now auto-enrolled as CodeSafe 5 clients if there is a `[codesafe]` configuration present (i.e. no need to configure this manually via serial CLI or `appliance-cli` nor run `hsmadmin` enrollment as `root`). Auto-enrollment requires 13.7 nShield 5c image as well as Security World software.
- Developer ID certificates are loaded automatically from a designated directory `/opt/nfast/kmdata/cscerts` (Linux) or `C:\ProgramData\nCipher\Key Management`

`Data\cscerts` (Windows) if not already loaded The `PublishedSEEWorld` Java class can now be used to send SEEJobs to a CodeSafe application of any model that has had its SEE World ID registered as a published object.

- For any client library language, using published objects is the most convenient way to use a CodeSafe application with SEEJobs, and this is agnostic of the module type when using the `config` file to load the application and register it as a published object (via the `worldid_pubname` field in a `[codesafe]` section for CodeSafe 5 or a `[load_seemachine]` section for a previous models). The C and Java CodeSafe 5 examples have been updated to demonstrate this.

3.2.1.1. Breaking changes

The following breaking API and behaviour changes have been made:

- SEElib SEEJobs support for CodeSafe 5 has been moved to the `seelib.a` library in the CodeSafe SDK (the separate `liblegacy_compatibility.a` has been removed).
- The API is more consistent with SEElib for Solo XC and Connect XC, with `SEElib_init()` now initializing SEEJobs support on the default port of `8888` and the `SEElib_Legacy_Support_Init()` function has been removed
- It is possible to enable a non-default port for SEEJobs by calling `SEElib_SetPort(8000)` (for example) before `SEElib_init()`. To disable SEEJobs listening altogether, run `SEElib_SetPort(0)` before `SEElib_init()`
- The client-side `legacy-csee-host-side-compatibility.h` and `legacy-csee-host-side-compatibility.c` have been removed and are no longer supported for SEEJobs communication from the host.
- All SEEJobs communication must now be done via the `hardserver` using normal nCore commands, like was the case in CodeSafe for XC and previous HSM models, and the wire format differs from the one implemented by the CodeSafe-side `liblegacy_compatibility.a` that was present in previous releases.
- The `hardserver` automatically redirects `Cmd_SEEJob` and `Cmd_FastSEEJob` commands directed at a SEE World ID object loaded on nShield 5s or nShield 5c modules to the CodeSafe 5 application via the SSH tunnel when it has been created automatically based on the `[codesafe]` configuration.
- The `SEEWorld5` Java class has been reained to support the `Cmd_CreateSEEConnection` part of the CodeSafe 5 setup (if not using published objects), but it uses the `hardserver` now for SEEJobs communication, the same as `PublishedSEEWorld` (and `SEEWorld` class for previous HSM models). The functionality in this class that used the protocol that was implemented by CodeSafe-side `liblegacy_compatibility.a` (and was the Java equivalent of `legacy-csee-host-side-compatibility.h`) has been removed.

3.2.1.2. Customer changes that may be required

- The updated `/opt/nfast/java/classes/nCipherKM-jhsee.jar` is shipped in the CodeSafe SDK as source code to be built with the customer application. The instructions in https://nshielddocs.entrust.com/security-world-docs/codesafe/example-see-machines.html#HelloWorldJava for extracting and compiling these sources should be followed with the new version.
- The updated `/opt/nfast/java/classes/nCipherKM.jar` is contained in the Security World (SecWorld) software and should be used in conjunction with this.
- CodeSafe-side C code should delete any call to `SEElib_Legacy_Support_Init()` and link against `seelib.a` but not liblegacy_compatibility.a` which has been removed
- Host-side C applications using SEEJobs should stop referencing `legacy-csee-host-side-compatibility.h` and `legacy-csee-host-side-compatibility.c` and send `Cmd_SEEJob` (no timeout) or `Cmd_FastSEEJob` (2 minute timeout) commands in the normal manner via the `hardserver` nCore connection (e.g. using `NFastApp_Transact()` or `simple_transact()` etc.)
- If automatic loading of developer ID certificates is wanted, the certificates should be copied to the `/opt/nfast/kmdata/cscerts` directory on the client machine where the CodeSafe app is being loaded.
- Automatic enrollment of the client machine with CodeSafe 5 on the 5c requires that the client be configured as privileged, and that a v13.7 5c image is in place.
- Customers should ensure that their `network-conf.json` rules only allow communication via the `ssh_tunnel` and not via the (plaintext) `incoming` ports if they want to restrict communication to the SSH tunnel only. This may not have been clear in previous documentation and examples. The below example shows what this looks like for a CSEE (SEEJobs) application.

```
{
        "incoming": {
                "tcp":
                {
                        "protos": ["ipv6"],
                        "ports": []
                }
        },
        "outgoing" : {
                "tcp" :
                {
                       "protos": ["ipv6"],
                       "ports": []
                }
        },
        "ssh_tunnel" : {
                 "container_port" : 8888
        }
}
```

3.2.2. Configuration File

A new configuration section [codesafe] is now supported in the client-side harderver config file which allows specification of:

- the `esn` of the nShield 5s or nShield 5c module onto which to load the application the CodeSafe 5 `image_file` to load and run (this must be readable by the `nfast` user (which is a member of `nfast` group and `nfastadmin` group by default)
- the `worldid_pubname` to assign the published object that the SEE world ID is registered with

Run `cfg-mkdefault -f config.example` to create a new example config file showing this section.

You can manually add it to your existing config file before the `[load_seemachine]` section.

Example CodeSafe configuration entry

```
[codesafe]
# Start of the codesafe section
# The CodeSafe 5 applications to load and start on an nShield 5. Use
# [load_seemachine] for previous HSM types.
# Each entry has the following fields:
#
# ESN of the module to load the CodeSafe application onto
#  esn=ESN
#
# Whether this configuration entry is enabled (default="yes"). This is a
# convenience for disabling CodeSafe auto-loading on a given module
# temporarily without removing the configuration.
#  enabled=ENUM
#
# The filename of the CodeSafe application for this module to host.
#  image_file=STRING
#
# Port in the CodeSafe application that is configured for SEEJobs
# communication. An SSH tunnel is automatically created for SEEJobs
# communication between the hardserver and this port. Set to 0 to explicitly
# disable. (default=8888)
#  seejobs_port=PORT
#
# Enable ncoreapi access for the CodeSafe application with
# Cmd_CreateSEEConnection. The identities in the image_file are passed
# automatically. (default="yes")
#  enable_ncoreapi=ENUM
#
# The PublishedObject name to use for publishing the KeyID of the started
# CodeSafe application.
#  worldid_pubname=STRING
#
# Enable auto-enrollment of the client with an nShield 5c. Auto-enrollment is
# enabled by default. This setting is ignored if the HSM is an nShield 5s or
# if this machine is an unprivileged client of a 5c.
#  auto_enroll=ENUM
#
# Unless set to "no", logging will be enabled for the CodeSafe application
# (default="yes"). Logs can be retrieved with csadmin log get -u UUID
#  logging=ENUM
```

```
#
# If set to "yes", the CodeSafe application is forcibly re-loaded even if a
# matching image appears to be loaded already (default="no")
#  force_reload=ENUM
#
# Key names of identities of CodeSafe application to pass to
# Cmd_CreateSEEConnection. This is only applicable if enable_ncoreapi has not
# been disabled. If only signed with the ASK, this is passed, if signed with
# the ASK and one extra signature (csadmin image signextra) then the default
# is to pass only the extra identity, and if there are more signers than this
# then all the identities are supplied. To override the defaults (e.g. to
# supply both the ASK and signextra identies) specify the key names as a
# space-separated list. Note, this controls what is reported by
# Cmd_GetWorldSigners instead of the CodeSafe application.
#  identities=STRING
```

Entries for additional modules may be added separated by `----` lines.

A new or modified configuration or CodeSafe app can be applied to a module dynamically by running `nopclearfail -c -m MODULE_NO`. The new configuration or changed application will be loaded automatically after the module returns from the clear operation.

3.2.2.1. Automatic Startup

The configuration-helper program `hsc_codesafe` is run automatically by the hardserver during module startup (or after clear) to process this configuration, including the following steps:

- Automatically configures CodeSafe 5 on the 5c and enrolls it with the local system (requires 13.7 or later Connect image, and will be skipped if the client is not privileged, in which case it will have to be configured up-front manually to allow access to the unprivileged client).
- Stops all existing CodeSafe applications on the module.
- Destroys any existing CodeSafe applications on the module if they do not match the hash of the one specified in configuration.
- Loads any required developer ID certificates from the `/opt/nfast/kmdata/cscerts` directory (if not already loaded).
- Loads the CodeSafe application specified in config (if not already loaded).
- Enables CodeSafe logging in the application configuration.
- Enables the SSHD in the application configuration, gets the SSHD server public key, generates an ephemeral client key and registers it with the SSHD server (This is done for SEEJobs support unless `seelibs_port` is explicitly disabled).
- Starts the CodeSafe application.
- Runs the internal nShield `ncssh` tool to set up a mutually authenticated tunnel between a local UNIX domain socket that is accessible to the `hardserver` and the port (by

default 8888) for the SEEJobs protocol in the CodeSafe application.

- Runs Cmd_CreateSEEConnection with the identity information for the CodeSafe application (unless enable_ncoreapi is disabled).
- If worldid_pubname is set, runs Cmd_SetPublishedObject to register the SEE World ID returned by Cmd_CreateSEEConection so that applications can make use of the CodeSafe application (this ID should be used with calls to Cmd_SEEJob / Cmd_FastSEEJob).

hsc_codesafe will run until the module is cleared or the hardserver is shut down.

If the module is cleared, hsc_codesafe will be re-run automatically when it returns from clear to negotiate a fresh mutually authenticated SSH tunnel and start the CodeSafe application again.

Note that it takes a couple of minutes for the CodeSafe application to be available after the module is cleared. Loading performance will be improved in the next firmware release after this one.

3.2.2.2. Debugging startup configuration

In order to support build, run, debug cycles when the user is developing the CodeSafe 5 application, hsc_codeafe can also be run interactively without configuration in config and without needing to clear the module.

It can be passed the same name-value pairs of config entries on the command-line as would normally be read from the config file.

For example, to load a CSEE (SEEJobs) CodeSafe application, and then when it is ready, run a host-side command which uses the application:

```
hsc_codesafe -m1 image_file=/opt/nfast/custom-seemachines/echo.cs5 worldid_pubname=echosee -- perfcheck
"misc:SEEJob" -s -t 10
```

To load a non-SEEJobs application pass seejobs_port=0, and to prevent Cmd_CreateSEEConnection being run automatically pass enable_ncoreapi=no. The example below shows this, and just runs csadmin list to fetch the container address when loading has completed instead of running an application directly. In this example, the module to use is specified via ESN rather than via module number (either option is supported regardless of other parameters passed).

```
hsc_codesafe esn=8ED1-2C9A-9331 image_file=/opt/nfast/custom-seemachines/seetickets_netsee.cs5 seejobs_port=0
enable_ncoreapi=no -- csadmin list
```

3.2.2.3. Monitoring Connection Status

The log messages from `hsc_codesafe` are currently included in the `hardserver` log `/opt/nfast/log/hardserver.log` (or Event Log on Windows, can be retrieved on the command-line using `nshieldeventlog -c 10` for the last 10 lines, for example).

A "pseudo-module" is registered in the hardserver for the CodeSafe application SEE Jobs endpoint and is visible when running enquiry -m 1001 as the counterpart for module 1 , enquiry -m 1002 as the counterpart for module 2, and so on. This will return InvalidModule if the `hsc_codesafe` processing has not run to completion and is only visible when the SSH tunnel is set up and `Cmd_CreateSEEConnection` has been run successfully to trigger the enrollment of the CodeSafe application for SEEJobs via the `hardserver`. The version details reported by the pseudo-module reflect the version of the CodeSafe SDK whose SEELib library code the CodeSafe application is linked against (not the HSM firmware version).

CodeSafe 5 pseudo-module `enquiry` example:

```
$ enquiry -m1001
Module #1001:
 enquiry reply flags  none
 enquiry reply level  Five
 serial number
 mode                 operational
 version              13.7.2
 speed index          20000
 rec. queue           120..250
 level one flags      none
 version string       13.7.2-85-90e580d1
 checked in           0000000067ca1f41 Thu Mar  6 22:18:41 2025
 level two flags      none
 max. write size      262152
 level three flags    none
 level four flags     ServerHasPollCmds HasLongJobs ServerHasLongJobs ServerHasCreateClient
 module type code     17
 module type          nShield CodeSafe 5 on nShield 5
 product name         CodeSafe 5
 device name          #1001 CodeSafe 5 SEE Jobs Endpoint for 8ED1-2C9A-9331
 hardware status      OK
```

Apart from running `enquiry` for the reporting, the pseudo-module should not be used for any other client operations in this release.

The pseudo-module is an implementation detail to help support reporting of status of the SEEJobs communication separate from the main module, and exact details may differ in future.

3.2.3. Troubleshooting

You can monitor the progress in loading the CodeSafe application with `tail -f /opt/nfast/log/hardserver.log` (or monitoring the Event Log on Windows)

Output from CodeSafe 5 loading will appear as log lines containing `Module #1 Startup` (or whichever module number), so `grep` can be used to filter to just these messages.

When the CodeSafe application has been loaded successfully a log line like the below will be reported, meaning that the application is now available for client communication (and the message provides some example commands for further diagnostics information):

```
2025-03-13 12:33:24 t00e774076f7f0000: Hardserver [FP]: Notice: Module #1 Startup: hsc_codesafe:INFO: READY: /opt/nfast/custom-seemachines/echo.cs5 running on 8ED1-2C9A-9331 (#1); SEE World ID published as echosee; csadmin log get -u da5c30a8-a302-4dff-bda6-d424d5749273 to retrieve logs; enquiry -m 1001 to check SEEJobs endpoint status
```

If loading fails, retry can be attempted by clearing the module (that is the main module, not the pseudo-module in the 1001+ range) or by restarting the client `hardserver` (`nFast Server` service on Windows).

3.2.3.1. Limitations

- nShield 5c v13.6 Connect image with v13.5 HSM firmware or v13.7 Connect image with v13.7 HSM firmware is required for CodeSafe support with this release. Only v13.7 is supported for CodeSafe auto-enrollment with the nShield 5c.
- The automatic configuration only supports port forwarding via the SSH tunnel between a UNIX domain socket used by the hardserver and TCP port `8888` in the Code-Safe application for SEEJobs. In a future release, additional configurability in relation to the networking will be offered.

3.2.4. Revised set of CodeSafe 5 system calls

The list of permitted system calls (syscalls) in CodeSafe 5 applications has been revised in the v13.7 firmware as follows:

- The following system calls are now allowed: `_newselect`, `alarm`, `clock_getres`, `clock_-nanosleep`, `dup3`, `epoll_create`, `epoll_ctl`, `epoll_pwait`, `epoll_wait`, `eventfd`, `execveat`, `faccessat`, `fallocate`, `fchdir`, `fchmodat`, `fchown`, `fchownat`, `fdatasync`, `flock`, `fstatfs`, `fstatfs64`, `fsync`, `ftruncate`, `getitimer`, `getpgid`, `getrusage`, `getsid`, `lchown`, `linkat`, `mkdirat`, `msync`, `newfstatat`, `nice`, `pipe2`, `preadv`, `preadv2`, `prlimit64`, `pselect6`, `pwrite64`, `pwritev`, `pwritev2`, `readlinkat`, `renameat`, `renameat2`, `rt_tgsigqueueinfo`, `sched_yield`, `sendfile`, `setitimer`, `setpgid`, `setpriority`, `setrlimit`, `statx`, `symlinkat`, `syncfs`, `times`, `truncate`, `unlinkat`, `utime`, `utimes` and `waitid`.
- The following system calls have been denied: `fcntl64`, `fstat64`, `getrandom`, `lstat64`, `mount`, `sched_get_priority_min`, `sched_getaffinity`, `set_robust_list`, `sigreturn` and

`stat64`.

Attempting to execute any system call that is not allowed will now return `-1` and set `errno` to `ENOSYS` (previous behaviour was to raise the `SIGSYS` signal).

See the *nShield Security World CodeSafe 5 v13.7.3 Developer Guide* for the full list of allowed system calls.

3.2.5. Support for additional signatures on CodeSafe 5 images

It is now possible to add additional signatures to CodeSafe 5 images using `csadmin image signextra`.

See the *nShield Security World CodeSafe 5 v13.7.3 Developer Guide* for further information.

3.2.6. Support for remote configuration of CodeSafe 5 on the nShield 5c

The `cs5` command in the nShield 5c Serial Console is now also available remotely to privileged clients of the 5c via the `appliance-cli` client tool.

Run `appliance-cli -m1 cs5` from a privileged client to see the command-line options (replacing `1` in `-m1` with the module number of the 5c in question).

If remote configuration of CodeSafe 5 is not wanted, this command can be disabled by setting `enable_remote_cs5=no` in the `[server_settings]` section of the 5c `config` file.

Note that the `cs5` command now automatically changes to Maintenance mode, and then returns to Operational mode, when that is necessary to make a configuration change.

3.3. ML-DSA Post-Quantum Algorithm firmware support (NSE-48336)

Security World v13.7 introduces support for the FIPS-204 ML-DSA signature scheme Post Quantum Cryptographic algorithm.

The following operations are available using this new algorithm:

- Key generation
- Signature

- Verification

This functionality is currently only available via nCore.

3.3.1. `PostQuantum` Feature enable on nShield Solo XC

A new feature flag has been added to the nShield HSM called `PostQuantum` which demonstrates that the HSM is capable of Post-Quantum cryptography. This feature is always on by default on the nShield 5s. However, this feature needs to be purchased on the nShield XC HSM to enable this algorithm to work.

3.4. FIPS 186-5 (NSE-48673)

A new Security World cipher suite ECp521mAES is now available in the new-world utility options. This cipher suite is compliant with latest revision of the FIPS 186-5 Digital Signature Standard, and the following restrictions apply:

- DSA key pair generation and signature generation are forbidden in FIPS 140 Level 3 mode. DSA signature verification is still permitted.
- Type 2 and older smart cards (also known as Gemplus MPCOS smart cards) are no longer accepted for ACS and OCS creation. These cards are being deprecated. We highly recommended using type 3 smart cards (also known as Remote Administration Ready or RA Ready smart cards) which offer a higher level of security.

The type of the module signing key (KML) can now be selected when a Security World is created and/or loaded using the `--kml-type` option with the `new-world` utility. This can result in better performances with a potential security trade-off.

3.5. FIPS-approved ECIES primitive (NSE-49786)

Security World v13.7 introduces support for a FIPS-approved ECIES primitive scheme and associated mechanisms which allow key material and other data to be wrapped to 256-bit security strength.

Key features of this change include:

- a new KAPrimitive
- enforcement of ECPublic or ECDHPublic for encryption keys
- enforcement of ECPrivate or ECDHPrivate for decryption keys

3.6. EdDSA updates for FIPS 186-5 support (NSE-33661)

The Ed25519 and Ed448 signature algorithms are now enabled in FIPS mode.

3.7. Disabled DSA signature generation in newer FIPS compliant security worlds (NSE-53230)

New FIPS-compliant security worlds in strict FIPS mode only will no longer permit new DSA signature generation. DSA signature verification is unaffected this change as are existing security world types and non-strict-FIPS configurations.

3.8. Elliptic Curve MQV added by default (NSE-61279)

Security World v13.7 introduces a change in firmware which enables the Elliptic Curve MQV feature by default upon the successful completion of a firmware upgrade operation to the 13.7.1 firmware. This change applies to nShield Solo XC and nShield 5s module types.

3.9. Delivery of RSA and AES keys to Global Platform Cards (NSE-56996)

RSA and AES key types can now be delivered to smartcards that support the Global Platform specification.

3.10. ckcerttool needs EC cert import (NSE-25478)

ckcerttool now imports certificates for any private key. There is an option to set CKA_ID if it is not set on the private key. The label option no longer overrides an existing label on the pri vate key.

3.11. Reloadable PKCS#11 session keys (NSE-61666)

PKCS#11 Session keys and token keys are now able to be reloaded when running HA preload.

3.12. On/Off key generation functionality for PKCS#11 session keys (NSE-61072)

Security World v13.7 introduces a new PKCS#11 variable: `CKNFAST_SESSION_TO_TOKEN`

When set (the default) C_CopyObject is able to convert a session key to token key. Unsetting this variable allows faster generation of session keys, but disables the ability to convert a session key to a token key. This variable should be set if using a JCE PKCS#11 provider (e.g SunPKCS11) to generate persistent keys.

3.13. Support for foreign SEE Integrity Keys (NSE-20254)

Support for foreign SEE Integrity Keys has been added to nfkmverify and generatekey.

When verifying a key protected by a foreign seeinteg key the --trusted-certifier option may be supplied to nfkmverify to specify the hash of the seeinteg key.

The verification process will assume that the seeinteg key is good.

When generating a key protected by a foreign seeinteg key the hash of the seeinteg key may be supplied via the --trusted-ceritfier option or interactively.

Verification will not check the seeinteg key with the specified hash.

3.14. Linux RPM updates (NSE-67319)

Security World v13.7 introduces new functionality to RPMs.

This new functionality includes:

- Inclusion of a new set of driver packages for nShield Solo XC and nShield 5s module types.
- Building of driver packages during the RPM installation process.
- Running the nShield install scripts and validating the hardserver has started after the installation of RPM packages.

Refer to the user documentation for more information regarding these changes.

4. Deprecated and discontinued features

The following features are deprecated or discontinued in Security World v13.7. If you have been using these features, plan for a new configuration and workflow that does not make use of the feature:

- KeySafe
  This is the legacy Java application. **KeySafe 5** continues to be supported in v13.7. KeySafe information has been removed from the user documentation for v13.7 and later releases. Previous user documentation releases that cover KeySafe continue to be available at https://nshielddocs.entrust.com/.

5. Firmware images

5.1. nShield 5s firmware

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

- Primary Image
- Recovery Image
- Bootloader

The v13.7 release only updates the Primary image. The Recovery image and Bootloader can be kept at previously released versions.

Details on what the components are used for and how to upgrade the different components are detailed in Upgrade nShield 5s HSM Firmware. Read this section prior to upgrading any nShield 5s.

5.1.1. nShield 5s firmware

Type	Version	Description	Directory	VSN
Latest	13.7.1	Latest firmware with features from v13.7 release.	`firmware/nShield5s/latest/nShield5s-13-7-1-vsn4.npkg`	4

5.2. Solo XC firmware

Type	Version	Description	Directory	VSN
Latest	13.7.1	Latest firmware with features from v13.7 release.	`firmware/SoloXC/latest/soloxc-13-7-1-vsn37.nff`	37

5.3. nShield Edge Firmware

There is no updated nShield Edge firmware being made available with the v13.7 release.

6. Connect images

The nShield firmware and Connect Image ISO includes v13.7.1 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
Latest	13.7.1	13.7 nShield 5c image with latest 13.7 firmware	13.7.1	`nethsm-firmware/latest-all-13-7-1-vsn32/`	32

6.3. Connect XC images

Type	Version	Description	Firmware included	Directory	VSN
Latest	13.7.1	13.7 Connect XC image with latest 13.7 firmware	13.7.1	`nethsm-firmware/latest-all-13-7-1-vsn32/`	32

7. Upgrade from previous releases

7.1. Install 13.7.3 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 intermedi ate 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 configura tion is not compatible (either through current version or after upgrading to a newer version of the firmware). Please contact nshield.sup-port@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 v13.7.3 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.

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": "13.7.1-60-29caa782",
"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-13-7-1-vsn4.npkg --esn module-esn
```

and for recovery:

```
hsmadmin upgrade nshield5s-recovery-13-5-0.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.

7.4. 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)
- nShield 5c (Base, Mid, High)
- Connect XC (Base, Mid, High, Serial Console)

8.2. Supported operating systems

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

Operating System	Solo XC	nShield 5s	Connect XC, nShield 5c
Microsoft Windows 10 x64	Y	Y	Y
Microsoft Windows 11 x64	Y	Y	Y
Microsoft Windows Server 2019 x64	Y	Y	Y
Microsoft Windows Server 2022 x64	Y	Y	Y
Microsoft Windows Server 2022 Core x64	Y	Y	Y
Microsoft Windows Server 2025 x64	Y	Y	Y
Red Hat Enterprise Linux 8 x64	Y	Y	Y
Red Hat Enterprise Linux 9 x64	Y	Y	Y
SUSE Enterprise Linux 12 x64	Y	Y	Y
SUSE Enterprise Linux 15 x64	**N**	Y	Y
Oracle Enterprise Linux 8 x64	Y	Y	Y
Oracle Enterprise Linux 9 x64	Y	Y	Y

Security World v13.7.3 support is restricted to the x64 architecture. Additional mainstream 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
17	Y
21	Y

8.3.2. Python

This lists the versions of Python that are supported.

Version	Supported
3.11	Y

8.4. Supported hypervisors and virtual environments

Operating System	Solo XC	nShield 5s	Connect XC, nShield 5c
Microsoft Hyper-V Server 2016	Y	N	Y
Microsoft Hyper-V Server 2019	Y	N	Y
Microsoft Hyper-V Server 2022	Y	N	Y
VMWare ESXi 7.0	Y	N	Y
VMWare ESXi 8.0	Y	N	Y
Citrix XenServer 8.2	Y	N	Y

8.5. Supported compilers for Microsoft Windows C developers

Security World v13.7.3 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
2022	Y

9. Known and fixed issues

Reference	Scope	Status	Description
NSE-69520	Client-side	Resolved	Fixed an issue on Windows where perfcheck called the deprecated Windows wmic tool, which may no longer be installed, to query CPU information for its report. **Resolved** in 13.7 client-side.
NSE-69076	Client-side	Resolved	Improved the CodeSafe 5 crash reporter so that some information would be provided even when a full backtrace was not available. **Resolved** in 13.7 client-side.
NSE-69020	Connect	Open	An issue currently exists where the Connect 5c upgrade will fail to upgrade if the time is not set on the module. Refer to Unset module RTC upgrade issue on Connect 5c units for more information. **Issue first found** in 13.6.
NSE-68179	Client-side	Resolved	Fixed an issue on Windows where an unwanted message box could appear relating to the TVD driver installation during a Security World software or Remote Administration software installation. **Resolved** in 13.7 client-side.
NSE-68044	Client-side	Resolved	Addressed an issue where the csadmin utility failed to include the scope ID when reporting link-local addresses. **Resolved** in 13.7 client-side.
NSE-68007	Client-side	Resolved	Fixed an issue where incorrect parameters in client nCore commands (like wrong module number) were unnecessarily reported as errors in the hardserver log. **Resolved** in 13.7 client-side.

Reference	Scope	Status	Description
NSE-67930	Client-side	Resolved	Fixed an issue where CodeSafe 5 CSEE (SEElib) applications could fail with SIGPIPE in some cases. **Resolved** in 13.7 client-side.
NSE-67846	Client-side	Resolved	Fixed an issue where the nShield Audit Service could fail to correctly resume handling the export and expiry of system logs where an interruption had occurred during export on a previous run. **Resolved** in 13.7 client-side.
NSE-67601	Firmware	Resolved	Addressed an issue where the incorrect BIOS code would be reported when the VCM would fail to start in single-tenant mode. **Resolved** in 13.7 firmware.
NSE-67579	Client-side	Resolved	Fixed an issue where output from nshieldaudit when printing to stdout rather than to file was not in JSON format as intended. **Resolved** in 13.7 client-side.
NSE-66905	Documenta-tion	Resolved	The documented set of allowed CodeSafe 5 system calls now reflects the set of system calls allowed by seccomp. **Resolved** in 13.7 documentation.
NSE-66437	Connect	Resolved	Made the Connect CLI command `setminvsn` more user-friendly. **Resolved** in 13.7 Connect images.
NSE-66432	Connect	Resolved	Addressed an issue with `hsmdiagnose` where a test was incorrectly skipped. **Resolved** in 13.7 Connect images.

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-66256	Client-side	Resolved	Addressed an issue where the message "Failed to parse last log data from current log" would be displayed in the nshieldaudidtd logfile. **Resolved** in 13.7 client-side.
NSE-66232	Firmware	Resolved	Addressed a firmware issue which prevented CodeSafe 5 CSEE machines built with 13.4 SDK from working on later versions of firmware. Applications built with 13.4 SDK will work on 13.7 and later firmware, but they cannot run on 13.5 firmware which does not have this fix. **Resolved** in 13.7 firmware.
NSE-65799	Client-side	Resolved	Addressed an issue where a stack trace would be displayed during installation on SLES12 platforms. **Resolved** in 13.7 client-side.
NSE-65292	Firmware	Resolved	Addressed an issue where a Status_Failed message would occur instead of Status_DecryptFailed with RSAUnwrap and AES Key unwrapping under certain circumstances. **Resolved** in 13.7 firmware.
NSE-65229	Firmware	Resolved	Addressed an issue where DeriveMech_PublicFromPrivate doesn't work with Ed448Private. **Resolved** in 13.7 firmware.
NSE-65109	Firmware	Resolved	Addressed an issue where the Solo XC was too enthusiastic to clear the module from the clear button. **Resolved** in 13.7 firmware.

Reference	Scope	Status	Description
NSE-64885	Client-side	Resolved	Addressed an issue where the CONNECTION ERROR: Unable to connect to 'monitor' failure would occur when multiple clients were attempting to connect to the monitor service. **Resolved** in 13.7 client-side.
NSE-64885	Documentation	Resolved	Addressed an issue where the M_AESmGCM HTML docs omitted the ciphertext format. **Resolved** in 13.7 documentation.
NSE-64438	Firmware	Resolved	Addressed an NVMWearLevel issue for Solo XC and nShield 5s units. **Resolved** in 13.7 firmware.
NSE-63892	Client-side	Resolved	Addressed an issue where generated nCore HTML pages could be missing. **Resolved** in 13.7 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	Addressed an issue in PKCS#11 where the following error would be reported: 'Key generation certificate with no private/secret key?' **Resolved** in 13.7 client-side.

Reference	Scope	Status	Description
NSE-63444	Client-side	Resolved	Addressed an issue in PKCS#11 where a mixing up of key type enums cause a 'NFBER_Encode_Octet_BitStr_Key failed for len' error. **Resolved** in 13.7 client-side.
NSE-62533	Client-side	Resolved	Addressed an issue in PKCS#11 where SELinux would prevent CodeSafe 5 SEE Machines from binding on some ports. **Resolved** in 13.7 client-side.
NSE-61967	Client-side	Resolved	Addressed an issue where the tar utility would be killed by seccomp when used within a CodeSafe 5 application. **Resolved** in 13.7 client-side.
NSE-61540	Client-side	Resolved	Addressed an issue where the CS5 Compatibility Layer would not stay listening for incoming connections. **Resolved** in 13.7 client-side.
NSE-61148	Firmware	Resolved	Addressed an issue where the init log is not created by replacement Python code as it should be. **Resolved** in 13.7 firmware.
NSE-61033	Firmware (5s only)	Resolved	Addressed an issue where deprecated options were reported in the nShield 5s system logs. **Resolved** in 13.7 nShield 5s firmware.
NSE-60936	Firmware	Resolved	Addressed an issue where Codesafe can lose trace data. **Resolved** in 13.7 firmware.

Reference	Scope	Status	Description
NSE-60554	Client-side	Resolved	Addressed an issue where TUAK and Milenage session key generation performance had decreased due to the need to generate key generation certificates at the point of key generation. This has been resolved by adding a new PKCS#11 environment variable: CKNFAST_SESSION_TO_TOKEN, this is enabled by default. The default behaviour is to generate session keys without Key Generation Certificates. This can be disabled by setting CKNFAST_SESSION_TO_TOKEN=0. **Resolved** in 13.7 client-side.
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
NSE-55428		Open	Building classic Codesafe examples fails with older compiler. **Issue first found** in 13.4
NSE-55425	Firmware	Resolved	Addressed an issue where 'Unable to perform operation due to service interdependency lock' was reported when using the `csadmin` utility. **Resolved** in 13.7 firmware.
NSE-55378		Open	Minor inconsistency when enabling autostart via csadmin config.
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-52456	Firmware (5s only)	Resolved	Addressed an issue where hsmadmin settime would leave the module around 2 seconds behind the host. **Resolved** in 13.7 nShield 5s firmware.

Reference	Scope	Status	Description
NSE-48991	Client-side	Resolved	Addressed an issue where nfkmutils.loadkey did not support softcards. **Resolved** in 13.7 client-side.
NSE-43472	Client-side	Resolved	Addressed various issues with nfkmutils.loadkey. **Resolved** in 13.7 client-side.
NSE-42031	Firmware (XC only)	Resolved	Addressed a gradual increase in memory usage on nShield Solo XC modules. **Resolved** in 13.7 nShield Solo XC firmware.
NSE-41205	Firmware (XC only)	Resolved	An issue has been fixed that can cause a Solo XC or Connect XC HSM to enter an SOS state after many days of running. The issue would have generally manifested as an SOS-HV or SOS-HRTP, but other SOS codes are possible. A number of "SpiRe-tries" as reported by stattree utility may precede the failure. **Resolved** in 13.7 nShield Solo XC firmware.
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-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-36086	Client-side	Resolved	Addressed an issue where OpenSSH did not enable TCP_NODELAY resulting in latency spikes in CodeSafe 5 communica-tion. **Resolved** in 13.7 client-side.

Reference	Scope	Status	Description
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-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-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-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