Application Notes

nShield 5 Adoption Guide

07 October 2024

Table of Contents

1. Introduction

Entrust introduced a new nShield HSM family, called the nShield 5, in 2022. It was released in two form factors, a PCI-e card called the nShield 5s, and a network attached unit called the nShield 5c. These HSMs are replacements for the nShield Solo XC and nShield Connect XC HSMs, respectively.

nShield 5s received both the FIPS 140-3 Level 3 and Common Criteria certifications. It supports all use cases of previous nShield HSMs and introduces new features.

This guide helps you plan and prepare to add nShield 5 HSMs to your existing Security World environment and transition from the Solo XC and Connect XC family to the nShield 5s and nShield 5c. It provides planning guidance and recommendations, and a collection of use cases, so you can ensure you maintain and meet your compliance objectives.

This guide is for customers with an existing Solo+, Solo XC, Connect+ and/or Connect XC HSM estate who want to adopt the nShield 5 into this environment.

1.1. nShield 5 compatibility

The nShield 5 HSM continues to use the same Security World Architecture as previous generations of nShield HSMs, allowing nShield 5 HSMs to work alongside existing HSM estates.

Importantly this means that Security Worlds created for previous generations of nShield HSMs can be loaded onto the nShield 5 HSM without any need for specific migration activities. Enrolling additional nShield 5 HSMs into the same Security World as other HSMs or transitioning from older HSMs to the nShield 5 is made easy by this common architecture.

The nShield 5 also shares a common firmware algorithm support and Security World restrictions (i.e. FIPS level 3 mode and cmts mode) as older generation HSMs. As such, the nShield 5 will continue to support the same algorithms and follow the same restrictions as that of an older generation HSM using the same version of firmware and Security World Software.

There are, however, a number of improvements made to the operation of the nShield 5 HSM that this document captures.

2. nShield 5 feature enhancements

2.1. nShield 5 Hardware

nShield 5s

The nShield 5s is a new HSM based on the PCIe form factor.

The hardware is similar to that of the nShield Solo XC with the following main differences:

- Fanless operation
- HSM mode switching is now under software control; the rear-panel mode switch and internal DIP switches have been removed
- The rear panel **Clear** button is repurposed as a **Recovery Mode** button
- Updated internal components including update to 8GB RAM
- The Status LED now displays simplified ("BIOS" style) error codes, replacing the Morse Code "SOS" codes. See HSM status indicators and error codes (nShield 5s).
- Recovery firmware

Both server and operating system compatibility was kept similar to that of the Solo XC, see hsm compatibility for more details of the support.

nShield 5c

The nShield 5c is a new network attached form factor HSM. Externally the nShield 5c will look very similar to the Connect XC, however internally the 5c has received a number of upgrades, namely:

- Updated processor
- Updated fans and new airflow ducting to support the nShield 5s
- Internal module is an nShield 5s

The nShield 5c comes with serial console as default.

2.2. Firmware architecture

The architecture of the nShield 5s firmware has been updated to be service oriented and container-based. This will allow for multi-layer security and a clear separation of roles, to support a future multi-tenant environment.

The nShield 5s exposes a number of different services which are divided into platform

services and the ncoreapi service. The `ncoreapi` service provides cryptographic services to the end user, whereas the platform services provide tasks associated with the installation, commissioning and maintenance of the HSM firmware and hardware. Each of the platform services and the `ncoreapi` service has its own communication channel with the host PC that is protected by use of SSH encryption.

The different services of the nShield 5 are described in more detail in Platform services.

Platform Management

The new nShield 5s Platform Services are administered through the unified utility `hsmadmin`, which directs the command to the service that implements the command. See `hsmadmin` for more information of the options provided by this new tool.

2.3. Host to nShield 5s communication

The communication protocol between the nShield 5s and the host has been updated to be based on the standard SSH protocol. To allow mutual authentication of the endpoints, the SSH protocol uses separate key pairs in the host and the HSM. You need to install the SSH keys for each nShield 5s service introduced above before you can use those services.

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

Firmware version v13.5 introduced additional enhancements making the SSH keys further protected by an internally generated certificate.

See setup ssh keys for more information about the use of SSH in the nShield 5s.

Because of this communication enhancement, the nShield 5s HSM cannot be moved from one machine/server to another. The SSH keys will have to be backed up and recovered on the new machine.

It is important to ensure the SSH keys are backed up, which can be done using the `hsmadmin` keys backup command. See backup for more information on the backup procedure.

The host still uses impath to communicate with the nShield 5c, same as the Connect XC.

2.4. nShield 5s firmware upgrade

The nShield 5s firmware consists of 3 major components:

- Primary image firmware
- Recovery image firmware
- Bootloader firmware

Unlike the Solo XC, upgrade packages are provided in the `.npkg` format and there is a different upgrade package for each of the different components. However the same upgrade procedure is used for upgrading all parts of the firmware.

See Upgrade firmware: nShield 5s for detailed information about the procedure for upgrading the firmware on the nShield 5s.

The nShield 5s continues to have a Version Security Number (VSN), same as the Solo XC. However enhancements to how this VSN can be used have been made. See nShield 5s VSN management.

2.5. nShield 5c upgrade

There are no differences to upgrade procedure of the nShield 5c as compared to the Connect XC.

2.6. nShield 5s VSN management

The nShield 5s introduces improvements to the management of the Version Security Number (VSN) enabling customer flexibility in setting the minimum 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. 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.

See firmware version control for more information.

2.7. nShield 5c VSN management

There are no differences to the VSN procedure of the nShield 5c as compared to the Connect XC.

2.8. nShield 5 modes of operation

The nShield 5s introduces differences to the HSM modes as compared to the Solo XC, including the addition of the new Recovery Mode which enables the return the HSM to a known good state for disaster recovery. Factory state operation also contains changes from that of the Solo XC all of which are detailed in operation modes.

On Windows, you have to run `hsmadmin enroll` after installation for the module to show in the `enquiry` output.

2.9. CodeSafe 5

The nShield 5s continues to support a Secure Execution Environment called CodeSafe, however this has been updated to take advantage of the changes made to the firmware architecture. As such, this is now called **CodeSafe 5**.

CodeSafe 5 introduces:

- Applications as container images

  In CodeSafe 5, the application is a container image, meaning a complete filesystem image that can contain multiple executables, libraries, scripts, and data files.

- Easy network connectivity

  nShield 5 HSMs and CodeSafe 5 containers are logically connected via TCP/IP networking. The container running the SEE Machine can receive incoming connections from the host side app, establishing two-way communication between host side app and SEE machine. Existing software that makes use of incoming or outgoing network connections can run with little or no modifications

- 'Secure by default' client communication

  The CodeSafe 5 execution environment includes both a configurable firewall and an SSH server. The firewall is set according to configuration in the signed CodeSafe 5 application package so that only the network ports required by the application are allowed. The SSH server allows a secure tunnel to be established to the CodeSafe 5 application. The client credentials required to access this tunnel can be configured using the support tools.

- Language support - the CodeSafe 5 SDK supports:
  - C and C++
  - Python 3

- CodeSafe 5 applications are now signed

  Requires the use of a developer ID.

For more information on the differences in the development and use of CodeSafe 5, see CodeSafe 5 User Guide.

Specific instructions exist to port existing see machines, which details migrating current Solo XC CodeSafe apps to CodeSafe 5.

2.10. nShield 5 logging

The nShield 5s (`ncoreapi`) continues to provide access to the same logging and diagnostics as the nShield XC, including the use of Audit logging.

Audit Logging

Audit Logging on nShield HSMs provides the means to log administrative operations and key usage events across your estate of HSMs. Audit logging was first introduced in Security World v12.60 on the nShield XC platform. nShield 5 continues to provide the same Audit Logging functionality.

However, in Security World v13.6 (on v13.5+ nShield 5s firmware) a new Audit Logging format was introduced, called **CEF audit logging**. This is detailed in in the user guide, see audit logging.

System Logs

The nShield 5s contains new System Logs that provide important logs generated by the platform services. Within this there are two different types of logs:

- init logs
- system logs

Both logs record information automatically and there is no user configuration required. The information recorded is determined by the system and there is no user configuration of the level of information recorded.

For HSMs running firmware version 13.5 or later the system logs are produced in a signed format. HSMs running firmware earlier than 13.5 produce logs in an unsigned format.

For information about how to retrieve and clear the logs, see system logging.

3. nShield 5 certifications

nShield 5 has FIPS 140 Level 3 and Common Criteria EAL4+ certifications, including QSCD status for eIDAS. This level of certification is equivalent to nShield XC.

3.1. FIPS 140-3

The nShield 5s is fully validated to FIPS 140-3 Level 3, FIPS cert. 4745. nShield XC has FIPS 140-2 Level 3 validation and will not be submitted for FIPS 140-3.

FIPS 140-3 is the latest revision of the FIPS 140 standard. It was made effective by NIST in September 2019 and accepted for new FIPS submissions one year later, in September 2020. All FIPS 140-2 certificates will be sunset and placed on the Historical list after September 22nd, 2026.

FIPS Level 3 mode and restrictions

The FIPS Level 3 mode in nShield 5 is equivalent to nShield XC. A FIPS Security World v3 created on nShield XC v12.50 or v12.72 validated firmware is fully compatible with the new FIPS 140-3 validated firmware 13.2 and 13.4 on nShield 5s.

3.2. Common Criteria

The nShield 5s is certified to Common Criteria EAL4 + AVA_VAN.5, ALC_FLR.2 using the Protection Profile EN 419 221-5, see the certification document. It also achieved QSCD status, relevant for the eIDAS regulation. This certification is equivalent to nShield XC.

4. Hardware, firmware, software versions in nShield 5

4.1. nShield Security World software

Entrust introduced support for the nShield 5 HSM in the v13.2 Security World release. To make use of the nShield 5 the Security World version needs to be at v13.2 or later.

All subsequent releases of v13.x include support for the nShield 5 and previous generation HSMs (nShield XC and nShield Solo+). All customers are recommended to use v13.6 of Security World clientside software irrespective of the nShield HSM in use. Using the v13.6 (or v13.3+) version makes the adoption of nShield 5 possible whilst still supporting current HSMs. The Security World loaded on the current Solo XC/Solo+ HSMs can be loaded on the nShield 5 HSMs.

The key Security World clientside versions are:

Release	Latest version	Release notes	Notes
13.2	13.2.2	v13.2.2	First released version of v13.x Security World, focused on providing support for the new nShield 5 product line No longer recommended to be used or supported.
13.3	13.3.2	v13.3	First v13.x release adding mainline support for nShield 5 HSM and including similar updates to the other nShield HSMs
13.4	13.4.5	v13.4.5	First release adding support for CodeSafe 5 on the nShield 5.
13.6	13.6.3	v13.6.3	Current latest Security World Release supporting all supported nShield HSMs and the latest feature set. Recommended version for use.

4.2. nShield 5s firmware

The following are key versions of the nShield 5s firmware:

Version	Latest version	Certification	Release notes	Notes	Solo XC equivalent
13.2	13.2.4	FIPS 140-3 FIPS cert. 4745	v13.2.4	First version of nShield 5s firmware FIPS 140-3 certified firmware	12.72.3

Version	Latest version	Certification	Release notes	Notes	Solo XC equivalent
13.3	13.3.1	Previous Latest	v13.3	Previous latest version of nShield 5s firmware adding new features but with no certification Upgrade to v13.5 firmware for new latest firmware is recommended	13.3.1
13.4	13.4.5	FIPS 140-3 FIPS cert. 4745	v13.4.5	Added support for CodeSafe 5 FIPS 140-3 certified firmware Recommended version of nShield 5s firmware to use if FIPS certification is required	12.72.3
13.5	13.5.1	Common Criteria CC cert link	v13.5.1	Common Criteria certified firmware Recommended version of nShield 5s firmware to use if Common Criteria certification is required	12.60.15
13.5	13.5.1	Latest	v13.5.1	Latest version of nShield 5s firmware Is currently the same as the CC approved version above	13.5.3

4.3. nShield 5c image

The following are key versions of the nShield 5c image.

As with Connect XC releases, each release contains multiple versions of nShield 5c images to provide versions with the different types of nShield 5s firmware.

Version	Latest version	Release notes	Notes	Connect XC equivalent
13.2	13.2.2	v13.2.2	First version of nShield 5c image No longer recommended to be used or supported; does not contain any currently certified nShield 5s firmware	12.80.5
13.3	13.3.2	v13.3	Previous latest version of nShield 5s firmware adding new features but does not contain latest certified 5s firmware Upgrade to v13.6 image for use with latest and certified firmware is recommended	13.3.2

Version	Latest version	Release notes	Notes	Connect XC equivalent
13.4	13.4.5	v13.4.5	First nShield 5c image adding CodeSafe 5 support for nShield 5 No longer recommended to be used or supported; does not contain any currently certified nShield 5s firmware	13.4.5
13.6	13.6.1	v13.6.3	Recommended version of nShield 5c image, which supports all versions of nShield 5s firmware (FIPS, CC and Latest)	13.6.1

5. nShield 5 adoption steps

The steps below detail the most common approach for adoption of the nShield 5, both the nShield 5s and the nShield 5c.

As detailed in nShield 5 Compatibility, the nShield 5 HSM will support the same algorithms and follow the same Security World restrictions as an older generation of HSM running the same version of firmware and using the same Security World Software. Please consult the firmware release notes for details of any changes to this from the version currently in use.

1. Upgrade Security World Clientside Software

   The first step is to ensure the clientside software has been upgraded to a version that supports the nShield 5 HSM:

   Upgrade the Security World Clientside software to the latest v13.6 version. See for detailed instructions on installing v13.6.

   After this step, the Security World will support current HSMs and nShield 5.

2. Install the new nShield 5 HSM hardware.

   Follow the hardware setup instructions to install the new nShield 5 HSM. See hardware install guide.

3. Upgrade the 5s firmware or 5c image to the required version. Upgrade the firmware on the nShield 5s and/or 5c image on the nShield 5c to the desired version.

   See Hardware, firmware, software versions in nShield 5 for details of the different versions and certifications and what new nShield 5 FW should be used.

4. Load/create new security world onto the nShield 5 HSM.
   - If a Security World already exists, load this onto the new nShield 5 HSM, see add an HSM to a security world.
   - Otherwise, create a new Security World onto the new nShield 5 HSM, see create a security world.