



ENTRUST

Release Notes

nShield Security World v13.5.1 Release Notes

Table of Contents

| | |
|---|---|
| 1. Introduction | 1 |
| 1.1. Purpose of Security World 13.5.1 | 1 |
| 1.2. Versions of these Release Notes | 1 |
| 2. Product versions | 2 |
| 2.1. nShield firmware version | 2 |
| 3. nShield 5s HSM Firmware | 3 |
| 3.1. nShield 5s Firmware Version Check | 3 |
| 3.2. Upgrading the nShield 5s Primary & Recovery Image | 3 |
| 3.3. Upgrading the nShield 5s Bootloader | 4 |
| 3.3.1. Pre-Requisites | 4 |
| 3.3.2. Upgrading bootloader | 4 |
| 4. Compatibility | 5 |
| 4.1. Supported hardware | 5 |
| 4.2. Supported operating systems | 5 |
| 4.3. API support | 5 |
| 4.3.1. Java | 6 |
| 4.3.2. Python | 6 |
| 4.4. Supported compilers for Microsoft Windows C developers | 6 |
| 5. Documentation | 7 |

1. Introduction

These release notes apply to release of version 13.5.1 of Security World Software for the nShield family of Hardware Security Modules (HSMs). They contain information specific to this release such as new features, defect fixes, and known issues.

The Release Notes may be updated with issues that have become known after this release has been made available. For the latest version, see the [Entrust nShield Support portal](#).

Access to the Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

1.1. Purpose of Security World 13.5.1

Security World version 13.5.1 introduces updated nShield 5s firmware specifically for Common Criteria certification.

1.2. Versions of these Release Notes

| Revision | Date | Description |
|----------|------------|---|
| 1.2 | 2024-06-11 | Terminology change from <i>firmware image version</i> to <i>firmware version</i> . No content change to the product or the Release Notes. |
| 1.1 | 2024-02-16 | Updated with firmware upgrade information |
| 1.0 | 2024-02-05 | Initial version |

2. Product versions

2.1. nShield firmware version

| Version | Description |
|---------|--|
| v13.5.1 | Release of 13.5.1 firmware for the nShield 5s HSM containing the latest features and fixes |

3. nShield 5s HSM Firmware

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

- Primary Image
- Recovery Image
- Bootloader

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 Common Criteria configuration. Details for upgrading the different components are detailed in the following section.

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
```

Following the 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",
```

If this is reported the nShield 5s is in a valid Common Criteria configuration.

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
```

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.

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.

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.

4. Compatibility

4.1. Supported hardware

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

- nShield 5s (Base, Mid, High)

4.2. Supported operating systems

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

| Operating System | nShield 5s |
|--|------------|
| Microsoft Windows 10 x64 | Y |
| Microsoft Windows 11 x64 | Y |
| Microsoft Windows Server 2016 x64 | Y |
| Microsoft Windows Server 2019 x64 | Y |
| Microsoft Windows Server 2022 x64 | Y |
| Microsoft Windows Server 2022 Core x64 | Y |
| Red Hat Enterprise Linux 7 x64 | Y |
| Red Hat Enterprise Linux 8 x64 | Y |
| Red Hat Enterprise Linux 9 x64 | Y |
| SUSE Enterprise Linux 12 x64 | Y |
| SUSE Enterprise Linux 15 x64 | Y |
| Oracle Enterprise Linux 7 x64 | Y |
| Oracle Enterprise Linux 8 x64 | Y |

Security World v13.5.1 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.

4.3. API support

4.3.1. Java

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

| Version | Supported |
|---------|-----------|
| 7 | N |
| 8 | Y |
| 11 | Y |
| 17 | Y |

4.3.2. Python

This lists the versions of Python that are supported.

| Version | Supported |
|---------|-----------|
| 2.7 | Y |
| 3.8 | Y |

4.4. Supported compilers for Microsoft Windows C developers

Security World v13.5.1 C libraries for Windows were built using Visual Studio 2017 and have been compiled with the SDL flag. This makes them incompatible with older versions of Visual Studio. This applies primarily to static libraries.

Microsoft Windows developers should upgrade to Visual Studio 2017.

5. Documentation

The documents in the 13.5.1 set are as follows:

- These *nShield Release Notes*
- [nShield 5s Install Guide](#)
- [nShield 5s User Guide](#)
- [nShield CodeSafe 5](#)



You can download these guides in PDF format [here](#).