nShield Security World (Multi-Tenancy)

nShield Security World v14.1.1 Release Notes

11 June 2026

Table of Contents

1. Introduction

These release notes apply to the release of version 14.1.1 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://trustedcare.entrust.com/. 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. Purpose of Security World v14.1

Security World version v14.1 introduces new features and enhancements as described in Features of Security World v14.1 STS Release 1. It also corrects a number of defects that have been identified in earlier releases.

Security World 14.1.1 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:

- nShield 5s firmware
- Security World Software

1.2. Versions of these Release Notes

Revision	Date	Description
1.0	2026-04-30	Release notes for the release of v14.1.1, Security World v14.1 STS Release 1.

2. Product versions

2.1. Security World software versions

Version	Date	Description
v14.1.1	2026-04-30	Full Release of the 14.1 Linux and Windows ISOs.

2.2. Firmware ISO versions

Version	Date	Description
v14.1.1	2026-04-30	Full Release of the 14.1 FW ISO including the updated 14.1 firmware.

2.3. nShield Firmware versions

Version	Date	Description
v14.1.1	2026-04-30	Full Release of 14.1 Firmware for the nShield 5s HSM containing the latest features and fixes.

3. Features of Security World v14.1 STS Release 1

3.1. Multi-tenancy

Security World v14.1 introduces a new Security World and nShield 5s firmware release that provides a significant new capability: `Multi-tenancy`.

Multi-tenancy enables the nShield 5s to create multiple isolated HSM instances (tenants), each running its own nCoreAPI instance. This allows multiple Security Worlds to operate on a single physical HSM and single firmware version. The Multi-tenancy architecture introduces the Service Provider and Tenant roles within an HSM deployment and requires updates to the architecture, deployment model, and administrative procedures.

For a detailed overview of Multi-tenancy including terminology, changes compared to non-Multi-tenant systems and example configurations, you should read v14.1.1@security-world-docs:mt-setup:intro.pdf prior to use.

By default, the firmware supports the creation of one single tenant only, allowing the HSM to operate in its traditional single-tenant mode and ensuring that the majority of existing use cases remain fully compatible. Applying a Multi-tenancy license enables the creation of additional tenants, unlocking the full Multi-tenancy feature set. All subsequent v14.x firmware releases will support both single-tenant and Multi-tenant deployment models.

This release focuses on introducing the core Multi-tenancy functionality. It is intended for customers who wish to deploy Multi-tenancy in the specific use cases detailed below. Additional Multi-tenancy capabilities are planned for future releases. The purpose of the v14.1 release is to allow customers to assess the new functionality and administrative model, and to understand how Multi-tenancy behaves within their own environments and deployment scenarios.

Security World v14.1 is an STS release and will not receive long-term support. Customers adopting Multi-tenancy should plan to upgrade to future releases that include additional enhancements and long-term maintenance.

Customers who do not intend to use Multi-tenancy should not install this release and should continue using their existing Security World version for the most up-to-date single-tenant capabilities.

Security World v14.1 STS Release 1 firmware is supported only when used with Security World v14.1 client-side software.

Downgrading: Customers who want to downgrade should first downgrade the firmware to the target release, then downgrade the client-side software to the same release after the firmware downgrade is com plete.

Downgrade from Security World v14.1 STS Release 1 has been tested to the following releases:

- Security World v13.9 STS Release 4
- Security World v13.6 LTS Update 6

Upgrading: Customers who want to upgrade should first upgrade the client-side software to Security World v14.1, then upgrade the firmware to v14.1.

Upgrade to Security World v14.1 STS Release 1 has been tested from the following releases:

- Security World v13.9 STS Release 4
- Security World v13.6 LTS Update 6

Post-downgrade/upgrade: After the module is returned to factory state, you must enroll it using the hsmadmin enroll command before per forming any other operations.

3.1.1. About the Multi-tenancy release

The Multi-tenancy capability has undergone extensive internal testing across specific scenarios and use cases.

Customers using Multi-tenancy in this release can expect:

- A secure and high-quality implementation of Multi-tenancy based on our latest platform improvements
- Broad compatibility with common use cases validated during pre-release testing
- The opportunity to identify edge cases or workflows unique to their environment

3.1.2. Use cases

Multi-tenancy on the nShield 5s is currently aimed at, and has been tested for, supporting

the following use cases:

3.1.2.1. Multiple Security Worlds on a Single HSM

The HSM runs a single Security World version at a time, but multiple, different Security Worlds (tenants) can be created. Tenants can be dynamically loaded or unloaded, enabling streamlined switching between Security Worlds.

This use case enables organizations to secure multiple Root Certificate Authorities (Root CAs) on a single HSM. By leveraging separate Security World domains, each Root CA's keys and operations are isolated with their own cryptographic domain and root-of-trust. This is built for offline Root CA use cases and high-assurance PKI deployments, allowing scalability and efficiency in protecting multiple Root CAs.

3.1.2.2. Multiple Virtual Machines Sharing One HSM

Multiple virtual machines running on the same host can be sharing a single HSM. In this model, the Service Provider creates a dedicated tenancy on the HSM for each virtual machine, allowing each virtual machine to operate its own isolated Security World.

3.1.2.3. Multiple Tenants Accessing the HSM Over a Local Network

The HSM is configured by the Service Provider to deliver cryptographic services over a LAN. Tenants operate on separate machines but share access to the HSM using their own isolated tenant environments. Currently, tenants are expected to reside on the same local subnet as the Service Provider.

Support for wider-area network topologies will be introduced in future releases, particularly with the planned introduction of Multi-tenancy support on the nShield 5c and nShield 5c 10G.

3.1.3. Known Limitations and notes of this release

This release has the following known limitations and notes:

- No support for Multi-tenancy on nShield 5c or nShield 5c 10G. Multi-tenancy is supported on nShield 5s only.
- No support for any hardware acceleration for any Post Quantum algorithms by the tenants
- CodeSafe 5 is not supported on v14.1 firmware, even when only a single tenant is con-

figured

- When deploying Multi-tenancy over a network, it is recommended that the Service Provider is hosted on Linux, due to the complexity of required network configuration.
- Network-resilience issues may be encountered, and tenants may occasionally need to perform manual intervention to reconnect to the Service Provider following network disruptions
- Only a single network connection is allowed per tenant
- Performance-management controls are limited. The HSM distributes performance across tenants and administrative operations on a best-effort basis. It is recommended that tenants be configured with Base or Mid performance settings.
- This release is focused on delivering functional Multi-tenancy under controlled and pre dictable load conditions. Issues may be encountered when operating the HSM at extreme load levels close to maximum HW resources, such as when running the maximum number of tenancies or applying heavy operational workloads. In this scenario it is expected that additional HSM units or dedicated single tenant HSMs should be used to provide the required performance.
- KeySafe 5 does not support the management of Multi-tenancy on the HSM.

3.2. nShield 5s in Virtual Environments (NSE-50078)

Security World v14.1 supports the use of nShield 5s units in Virtual Environments, refer to Supported hypervisors and virtual environments for more information on the supported plat forms.

A user should ensure that when performing a firmware upgrade of their nShield 5s unit in a Virtual environment they use the `--no-reset` command so that the module is not reset. Attempting to upgrade a nShield 5s unit in a Virtual Environment without using `--no-reset` will display an error.

Once the upgrade operation is complete the user **must** perform a restart of the Virtual Envi ronment physical host machine in order for the upgrade to be completed.

3.3. Open Source Software in the Security World v14.1 STS Release 1

Please consult the following documents on the ISOs for Open Source Software versions in the Security World v14.1 STS Release 1.

Component	PDF	ISO(s)
nShield 5s	5s-licenses.pdf	nShield_HSM_Firmware
Security World Software	secworld-licenses.pdf	SecWorld_Lin64 / SecWorld_Windows
Security World Software Python Packages	secworld-python-licenses.pdf	SecWorld_Lin64 / SecWorld_Windows / nShield-_HSM_Firmware

4. Firmware images

4.1. nShield 5s firmware

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

- Primary Image
- Recovery Image
- Bootloader

The v14.1 release contains a new v14.1 firmware for the nShield 5s. This new firmware 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.

4.1.1. nShield 5s firmware

Type	Version	Description	Directory	VSN
Latest	14.1.1	Latest firmware with features from v14.1 STS Release 1.	`firmware/nShield5s/latest/nShield5s-14.1.1-vsn5.npkg`	5

4.2. Solo XC firmware

There is no updated Solo XC firmware being made available with the v14.1 release.

4.3. nShield Edge Firmware

There is no updated nShield Edge firmware being made available with the v14.1 release.

5. Connect images

There are no updated Connect images being made available with the v14.1 release.

6. Upgrade from previous releases

6.1. Install 14.1.1 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.

6.2. Upgrade nShield 5s HSM Firmware

As detailed in the *nShield v14.1.1 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.

6.2.1. 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-MT",
"primary-version": "14.1.1-150-61f72278",
"recovery-version": "13.5.0-0-e2ec16eefd",
"uboot-version": "1.4.1-0-edb84d6e",
```

6.2.2. Upgrading the nShield 5s Primary

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 image can be upgraded using the following command:

```
hsmadmin upgrade nShield5s-14.1.1-vsn5.npkg --esn module-esn
```

7. Compatibility

7.1. Supported hardware

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

- nShield 5s (Base, Mid, High)

7.2. Supported operating systems

This release has been tested for compatibility with the following operating systems. As stated in the Known Limitations and notes of this release section, it is recommended that the service provider be hosted on Linux because of the complexity of the networking setup.

Operating System	Service Provider Support	Tenant Support
Microsoft Windows 11 x64	N	Y
Microsoft Windows Server 2022 x64	N	Y
Microsoft Windows Server 2022 Core x64	N	Y
Microsoft Windows Server 2025 x64	N	Y
Red Hat Enterprise Linux 8 x64	Y	Y
Red Hat Enterprise Linux 9 x64	Y	Y
SUSE Enterprise Linux 15 x64	Y	Y
Oracle Enterprise Linux 8 x64	Y	Y
Oracle Enterprise Linux 9 x64	Y	Y

Security World v14.1.1 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.

7.3. API support

7.3.1. Java

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

Version	Supported
17	Y
21	Y

7.3.2. Python

This lists the versions of Python that are supported.

Version	Supported
3.11	Y

7.4. Supported hypervisors and virtual environments

Operating System	nShield 5s
Microsoft Hyper-V Server 2025	Y
VMWare ESXi 8.0	Y

7.5. Supported compilers for Microsoft Windows C developers

Security World v14.1.1 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

8. Known and fixed issues

Also see Known Limitations and notes of this release for specific MT limitations of this v14.1 release.

Reference	Scope	Status	Description
NSE-77839	Firmware	Open	The system log entries that monitor VCM resource usage are overly verbose and in time can exhaust the disk space available on the HSM, resulting in system failure. To prevent this you should expire the logs on a regular basis. This can either be done manually or by use of the nShield Audit Log Service (nshieldauditd). See also NSE-77739. **Issue first found** in 14.1
NSE-75671	Client-side	Resolved	Removed the `pkcs11req` appname from `generatekey`. **Resolved** in 14.1 client-side.
NSE-75628	Client-side	Resolved	Addressed an issue where the `nethsmadmin` help menu was incomplete. **Resolved** in 14.1 client-side.
NSE-74960	Client-side	Resolved	Addressed an issue where `ulMinKeySize` and `ulMaxKeySize` was incorrect for multiple mechanisms for PKCS#11. **Resolved** in 14.1 client-side.
NSE-74381	Client-side	Resolved	Addressed an issue where an unnecessary public key import would occur in Java when calling `nCECDHKeyAgreement`. **Resolved** in 14.1 client-side.
NSE-74156	Client-side	Resolved	Addressed an issue where an assertion would occur when calling `perfcheck --diff` under certain circumstances. **Resolved** in 14.1 client-side.

Reference	Scope	Status	Description
NSE-74125	Client-side	Resolved	The slotinfo for loadshared slots now includes the `CKF_HW_SLOT` flag. Softcard slots may be distinguished from OCS slots by the `CKF_REMOVABLE_DEVICE` flag. **Resolved** in 14.1 client-side.
NSE-74083	Client-side	Resolved	Addressed and issue where Java PublishedSEEWorld's `getInitStatus()` method would throw a null pointer exception for already successfully initialised Worlds. **Resolved** in 14.1 client-side.
NSE-74078	Client-side	Resolved	Removed the `embed` key type from `generatekey`. **Resolved** in 14.1 client-side.
NSE-73380	Client-side	Resolved	Addressed an issue where WorkedExample.java would explicitly destroy keys by ID. **Resolved** in 14.1 client-side.
NSE-73324	Client-side	Resolved	`cklistvalues-dynamic` now returns CKA_PARAMETER_SET for ML-DSA keys. **Resolved** in 14.1 client-side.
NSE-73029	Client-side	Resolved	Addressed an issue that resulted in incompatibility between nShield 5 drivers and Linux kernel 6.16. **Resolved** in 14.1 client-side.
NSE-72542	Client-side	Resolved	Addressed an issue where `SEElib_StartProcessorThreads()` no longer crashes if nthreads is too high. **Resolved** in 14.1 client-side.

Reference	Scope	Status	Description
NSE-72539	Client-side	Resolved	Addressed an issue where `pending job table full` / `Status_ObjectNotReady` error from `SEElib_Transact()` no longer occurs when many hundreds of threads are created. **Resolved** in 14.1 client-side.
NSE-72389	Client-side	Resolved	Addressed an issue where a `Failed to add a watch for /run/user/0/systemd/ask-password: Permission denied` warning would be displayed during installation of the product, or during the hardserver start/stop process on Red Hat Enterprise Linux 10 x64. **Resolved** in 14.1 client-side.
NSE-72323	Client-side	Resolved	Addressed an issue where is was not possible to create an attestation bundle for various post-quantum key types. **Resolved** in 14.1 client-side.
NSE-72241	Client-side	Resolved	Addressed an issue where objects could leak in the Java CoreKey class. **Resolved** in 14.1 client-side.
NSE-71564	Client-side	Resolved	Addressed and issue where `nfkminfo` would use a backtick in the key name list output. **Resolved** in 14.1 client-side.
NSE-71427	Client-side	Resolved	The ppmk command's `--recover` option no longer requires the use of preload. **Resolved** in 14.1 client-side.
NSE-71392	Client-side	Resolved	Addressed an issue where `nfdiag` didn't include in the contents of the sbin directory in logfiles. **Resolved** in 14.1 client-side.

Reference	Scope	Status	Description
NSE-70765	Client-side	Resolved	Addressed an issue where `ncperftest` would not work with pre-created keys. **Resolved** in 14.1 client-side.
NSE-70375	Firmware (5s only)	Resolved	Addressed an issue with EllipticCurve ASN.1 inputs. **Resolved** in 14.1 firmware.
NSE-69888	Client-side	Resolved	The `nvram-sw --persistent` option has been extended to work with `--read`, `--write`, `--acl` and `--delete-noadmin`. **Resolved** in 14.1 client-side.
NSE-68682	Client-side	Resolved	Addressed and issue where `nethsmadmin --list-images` would return the wrong error message if the RFS IP was not specified. **Resolved** in 14.1 client-side.
NSE-64570	Client-side	Resolved	`nfkmattest` will now display the filename if a problem is encountered when reading the file. **Resolved** in 14.1 client-side.
NSE-62984	Client-side	Resolved	Addressed an issue in `nethsmadmin` where the feature file help was misleading. **Resolved** in 14.1 client-side.
NSE-60321	Client-side	Resolved	The default KNSO main-use timeout is now the maximum of 6 minutes per card, and 1 hour. The minimum is 3 minutes per card and the maximum is the greater of 10 minutes per card, and 2 hours. **Resolved** in 14.1 client-side.

Reference	Scope	Status	Description
NSE-60319	Client-side	Resolved	`nfkmverify` no longer reports a KNSO main use timeout longer than 10 minutes as a problem. The maximum permitted by `nfkmverify` is the greater of 10 minutes per card, and 2 hours. **Resolved** in 14.1 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-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.