Chapter

Release Notes: nShield Security World v12.40.2 Release Notes

Table of Contents

Chapter

1. Introduction

These release notes apply to version 12.40 of Security World Software, CipherTools, and CodeSafe for the nCipher 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.

Access to the Support Portal is available to customers under maintenance. Please contact nCipher at support@ncipher.com to request an account.

1.1. Purpose of this release

Security World version 12.40 introduces enhancements to versions s12.20 and v12.30 as described below, and corrects a number of defects that have been identified in earlier releases.

If you are using compatible nShield products covered by a current maintenance contract, you are eligible to upgrade the version of software and firmware that is used with these products.

We recommend you review this document to determine whether you should deploy version 12.40. **It is particularly important** that you read **Chapter 4: Upgrading from previous releases**.

For recent nShield Connect + and Connect XC purchases please refer to: **Important Addendum – New LCD Component, 31/1/2018** for up/downgrade considerations.

2. nShield v12.40.2

The v12.40.0 and 12.40.1 releases contain a number of issues that required an update:

1. A stability issue that could potentially cause a restart of the XC hardware

2. A performance issue that affects Solo XC when used in Linux based deployments and Connect XC
3. A CodeSafe issue that causes nCore commands to fail in SEE machines on Solo XC/Connect XC

This v12.40.2 release is a re-release of v12.40.1 addressing these issues. The issues affect all variants of the nShield XC hardware and both the FIPS and non-FIPS version. For customers on earlier versions of v12.40 we recommend customers upgrade to benefit from the improvements outlined below.

2.1. Changes in v12.40.2

The following changes have been made in the v12.40.2 release:

- Updated nShield Solo XC and nShield Connect XC firmware to address a stability issue that can cause a potential reset of XC hardware resulting in an "HSM Failed" error logged / displayed on front panel (NGSOL-2844). To resolve this issue Solo XC and Connect XC firmware version 3.3.21 has been updated and re-certified by NIST as version 3.4.1.
- Symmetric and asymmetric performance issues (NSE-11352) addressing a regression introduced in earlier v12.40.1 and 12.40.0 releases
    - Updated nShield Connect XC image files. These new image files have the version number 12.40.2 and include either the FIPS firmware or the latest firmware
    - Updated Linux driver included in new ISOs for Linux
- Updated ISOs for all operating systems to contain the updated nShield Connect XC images. The version number of these ISOs is now 12.40.2.
- Updated installers to contain the updated Connect XC images. The version number of these installers is now 12.40.2.

2.2. Changes in v12.40.1

The following changes have been made in the v12.40.1 release:

- Updated nShield Connect images containing a fix for the client licences issues. This image has the version number 12.40.1.
- Updated ISOs for all operating system to contain the updated nShield Connect image. The version number of these ISOs is now 12.40.1.
- Updated installers to contain the update Connect images. The version number of these installers is now 12.40.1.

- Updated installation guides and TVD guide to address minor issues found post 12.40.0 release.

2.3. Existing nShield Connect deployment with v12.40.0/v12.40.1 installed

If you already have v12.40.0 or v12.40.1 nShield software installed there is no need to uninstall this and install v12.40.2. There are no changes to the host side software.

The installation installs the Connect images into %NFAST_HOME%\nethsm-firmware directory and so a v12.40.0/ v12.40.1 installation will contain the older Connect images. These files must be manually updated by copying the Connect images from the ISO into that directory.

2.3.1. Installing the updated Connect image

There are no specific instructions for installing the updated Connect image (from either previous releases or if v12.40.0/v12.40.1 Connect image is installed). See the Appendix: Upgrading the nShield Connect image file and associated firmware in the nShield Connect User Guide for instructions on updating the Connect image.

The details of the new Connect image are available in “Chapter 4: Upgrading from Previous Releases”.

2.4. Existing nShield Solo and nShield Edge deployment with v12.40.0/v12.40.1 installed

If you already have v12.40.0 or v12.40.1 nShield software installed there is no need to uninstall this and install v12.40.2. There are no changes to the host side software.

2.5. Existing nShield Solo XC deployment in a Linux operational environment

If you already have v12.40.0 or 12.40.1 nShield software installed we recommend you uninstall this and install v12.40.2. to benefit from the performance and stability fixes listed above.

2.6. Existing nShield CodeSafe deployment for Solo XC or Connect XC

If you are using a CodeSafe installation for Solo XC or Connect XC please contact Support.

3. Main features of Security World v12.40

The main features introduced with v12.40 are as follows:

3.1. Integrated nShield XC support

Support for the new nShield XC (Solo XC and Connect XC) hardware platform was recently introduced in a number of special releases (s12.20.00, s12.20.50 and s12.20.51). These special releases supported the nShield XC only and were limited to Windows and Linux OS platforms. Security World v12.40 provides common support for all nShield HSMs: Solo XC, Connect XC, Solo, Solo+, Connect, Connect+, Edge, and nToken. This allows the same Security World software installation to work with a mixed estate of any nShield HSMs across the supported operating systems.

3.2. Additional Microsoft Windows OS support

Security World v12.40 adds in support for the following Microsoft Windows operating systems:

- Microsoft Windows 10 x64
- Microsoft Windows Server 2016 x64

Support for these two platforms uses the same nShield Windows installer as the other Windows OS installations.

3.3. Microsoft Windows Server 2016 Nano support

Security World v12.40 adds limited support for the Microsoft Windows Server 2016 *Nano Server* operating system.

The normal nShield installation media for Windows is not supported on Nano Server. There is a separate installation DVD for nShield Security World software for the Nano Server platform. This new DVD contains a document called “nShield_Installation_Guide_Nano.pdf” which provides the instructions for installing nShield Security World software on a Nano

Server and describes what Security World functionality is supported.

3.4. AIS-31 support

nShield Solo XC with firmware v12.40 now supports AIS-31 (BSI: Application Notes and Interpretation of the Scheme (AIS) 31 – Functionality Classes and Evaluation Methodology for Physical Random Number Generators).

3.5. DeriveKey ACLs

The `DeriveKey` nCore command introduces a new flag, `WorldHashMech`, which enables the use of the Security World hash mechanism in favour of SHA-1 hashes for key identification. ACLs may use the `Act_DeriveKeyEx` action (instead of `Act_DeriveKey`) to specify other keys, using the Security World hash mechanism. If the `WorldHashMech` flag has been set in the `DeriveKey` command, then `Act_DeriveKeyEx` must be used.

ACL verification can fail if `WorldHashMech` has been set and `Act_DeriveKey` is used.

The `GetKeyInfoEx` command now returns two hashes for a key object: SHA-1 and a stronger hash as determined by the Security World hash mechanism. This stronger hash is represented in the `KeyHashEx` structure, which also provides the mechanism used to generate the hash.

The Security World API (nfkm) supports building ACLs with `Act_DeriveKeyEx` through the introduction of the following functions: `NFKM_mkacl_derivekeyex` and `NFKM_mkacl_deriveroleidex`.

In this release this functionality is only available on the nShield Solo+ HSM. This omission will be addressed in a future release.

3.6. Default cipher suite

`DLf3072s256mRijndael`, which is SP800-131A compliant, is now the default cipher suite used when generating a Security World. Although this is now the default, users are still able to explicitly specify a cipher suite from the options available (e.g. through `new-world` using `--cipher-suite`).

Due to the additional primality checking required by SP800-131A, Security World generation and key generation operations will take longer

> when using the new default.

The deprecated `--km-type` option to `new-world` has been removed, `--cipher-suite` should be used instead. In addition, within `NFKM_InitWorldParams`, the `SetKMType` flag and `kmtype` parameter have been marked as deprecated.

3.7. SNMPv3 support

This release provides an SNMPv3 compatible agent that is a replacement for the SNMP agent in previous releases of nShield Security World software, which supported only SNMPv1 and SNMPv2c.

Security World v12.40 is directly compatible with CipherTrust Monitor 2.0 and greater.

3.8. SafeSign Cryptographic Module mechanisms

SafeSign Cryptographic Module support is implemented by an additional nShield specific API call and additional nShield specific mechanism, providing support for EMV Authentication and additional nShield specific mechanisms for the C_Verify and C_Sign standard PKCS#11 API calls in support of WatchWord/PSM authentication.

3.9. Deterministic ECDSA

Security World v12.40 latest firmware provides an implementation of deterministic ECDSA compatible with the UK specification GBCS 0.8.1 (note that this is not equivalent to RFC6979). This is currently only available through the nCore API.

This release does not support Deterministic ECDSA on nShield XC HSMs. This omission will be addressed in a future release.

3.10. Hyperledger support

Security World v12.40 provides a key derivation function based upon the Hyperledger client enrolment function. This is currently only available through the nCore API and the PKCS#11 API.

In this release only SHA2 is supported as the hashing function, and the mechanism is not available on nShield XC HSMs.

3.11. Versioning

From v12.40 onwards the way nShield software components are versioned has changed. This is in order to standardise the version numbers across the nShield software and firmware components. All host-side components, the firmware images, and the nShield Connect image, will have the same version number which will match the release version. This version number will be reported in the same way as previous releases (via enquiry, ncversions, the nShield Connect front panel, etc.).

Additional information is reported on these tools after the v12.40 version number, which is used to identify specific build information. This information is useful to reference when seeking support from nCipher. The “+” that is often reported immediately after the version number (i.e. “12.40.0+”) is used to show when the new version number is being used.

In v12.40 the version number of the Solo XC firmware is not currently consistent with the other components and for now will continue to follow the old versioning standard. This will be addressed in a future release.

As with previous nShield releases, Security World v12.40 also ships with older FIPS approved versions of the Connect images and associated firmware. The version numbers of these components have not been changed; they continue to be reported in the old version format.

The v12.30 nShield Connect image number is reported as "12.44.2cam15", which may appear to be a later version than the new version shipped with v12.40 (reported as “12.40.0+”). However as indicated by the "camX" and the lack of the “+” on the v12.30 version number, this is the old versioning standard. This shows that this version pre-dates the new “12.40.0+” Connect firmware version.

3.12. Firmware and nShield Connect image file

Security World v12.40 introduces new firmware for the Solo and Solo XC HSMs. The features that these HSMs support vary, which the table below describes. Functionality on the Solo HSM that is not on the Solo XC HSM will be addressed in a future release.

Feature	Solo/Solo+ Connect/Connect+	Solo XC Connect XC
Remote Administration (*introduced in v12.00*)	Yes	Yes
Pool mode (*introduced in v12.30*)	Yes	No
SafeSign Cryptographic Module mechanisms	Yes	Yes
Deterministic DSA	Yes	No
Hyperledger support	Yes	No
DeriveKey ACLs	Yes	No
AIS-31 support	No	Yes

Given the increased number of upgrade images available in v12.40, ensure the correct image version is used when upgrading.

4. Upgrading from previous releases

4.1. Installing v12.40 Security World software

Before installing this release, you must:

1. Confirm that you have a current maintenance contract that licenses you to deploy upgrades on each nShield HSM and corresponding client operating system
2. Uninstall previous releases of nCSS or Security World software, CipherTools, and Code Safe from the client machines
3. For Unix platforms, except Solaris 11, if you have applications built against previous versions of nflibs, in order to maintain backwards compatibility you must request the creation of the symlink /dev/nfast (which points to /opt/nfast/sockets) during the startup sequence.
    - To do this create the file /etc/nfast.conf with the entry NFAST_CREATEDEVNFAST=1

For details of how to install the v12.40 Security World software, refer to the Chapter: Installing the software, in the appropriate Installation Guide.

If the nShield Trusted Verification Device driver is installed as part of

> the installation the machine will need to be rebooted after the installation is complete.

4.2. Version Security Numbers

The following table shows the v12.40 VSN for different nShield HSMs:

HSM	VSN Change in v12.40	v12.40 VSN
nShield Solo, nShield Solo+ firmware	Yes	28
nShield Edge firmware	No	26
nShield Connect, nShield Connect+, nShield Connect XC image file	Yes	29
nShield Solo XC firmware	No	36

For security reasons, the VSN of the nShield Connect image file was increased to 29 and the VSN of the nShield Solo/Solo+ firmware was increased to 28. **Increasing the VSN ensures that once the nShield Solo/Solo+ Firmware or the nShield Connect image file from v12.40 has been installed, it is only possible to upgrade or downgrade to firmware or Connect image files with the same or a higher VSN**. Contact nCipher Support if you require further information.

4.3. Important Addendum – New LCD Component, 31/1/2018

Due to a hardware component change, the nShield Connect **image files** (and associated firmware) supplied with v12.40.2 and earlier software releases are incompatible with recently purchased nShield Connect hardware.

nShield Connect HSMs shipping with new LCD displays can be identified by checking the last character of the serial number label on the nShield Connect. Only Connect XC units with suffix F or greater and Connect
units with suffix D or greater are fitted with a new LCD. See table and figure below:

nShield Connect Model	Serial Number notation of nShield Connect with old LCD	Serial Number notation of nShield Connect on with new LCD
nShield Connect XC	36-XC*1234* **E**[1] and 46-XC*1234* **E**[1]	36-XC*1234* **F** and 46-XC*1234* **F**
nShield Connect+	36-MC*1234* **C**[2] and 46-MC*1234* **C**[2]	36-MC*1234* **D** and 46-MC*1234* **D**

Note 1 – Letter E or earlier units have older LCD component.

Note 2 – Letter C or earlier units have older LCD component.

See sample Connect XC product label located on the top of the unit indicating a unit with new LCD:

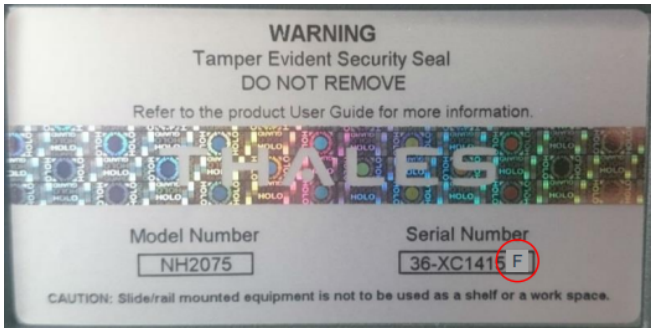

Figure 1: nShield Connect product label illustrating how to identify units with new LCD

nShield Connect units with new LCD (identified by the suffix on the unit serial number) are supplied preloaded with an image file (12.41.0cam4-fips) providing FIPS certified firmware. If you wish to upgrade the image file to a later, non-FIPS version, do not use the image files provided in v12.40.x or earlier releases. Please contact nCipher Support to request 12.41.0cam4 which is the latest compatible nShield Connect XC / Connect + image file.

4.4. Latest v12.40 HSM firmware and nShield Connect image

For details of how to upgrade HSM firmware, refer to Appendix: Upgrading firmware in the nShield Solo and nShield Edge User Guide, or Appendix: Upgrading the nShield Connect image file and associated firmware in the nShield Connect User Guide as appropriate.

The firmware is provided on the install media and should be installed on an nShield HSMs in accordance with Table 1. Table 1 details the directory location of the nShield firmware on the installation media, firmware and image file (for nShield Connect HSMs) and the

firmware versions supplied on the installation media.

If the HSM is not supported on the specific operating system the firmware will not be present.

Due to the VSN change on the nShield Solo/Solo+ HSM firmware, once the latest v12.40 firmware is installed by upgrading the Solo/Solo+ HSM it is not possible to downgrade to the FIPS approved firmware.

HSM	Directory location on the install media	VSN	Rollback possible?	Firmware version, FIPS status
nShield Connect nShield Connect+	nethsm-nShield firmware/12.40.2cam1/nCx3N.nff	29	N	12.40.0, won't be FIPS certified[1] [2] [3]
nShield Connect XC	nethsm-firmware/12.40.2cam1/nCx3N.nff	29	N	3.3.33, won't be FIPS certified[1] [2] [3]
nShield Solo nShield Solo+	Monitor: firmware/2-60-1/ldb_ncx3p-26.nff Firmware: firmware/12-4000/ncx3p-28.nff	28	N	12.40.0 Won't be FIPS certified[1] [2]
nShield Edge	Monitor: firmware/2-50-16/ldb_ncx1z-24.nff Firmware: firmware/2-652/ncx1z-26.nff	26	Y	2.65.2 Won't be FIPS certified[1]
nShield Solo XC	firmware/3.3.33/ncx5e-36.nff	36	Y	3.3.33 Won't be FIPS certified[1]

Table 1: Latest firmware and image files provided on v12.40 install media

Note 1: Functionality introduced in this firmware will be rolled into a subsequent firmware release and submitted for FIPS certification.

Note 2: Once installed, due to the VSN change, it will not be possible to downgrade to a previous version of firmware.

Note 3: nShield Connect units with new LCD (See Addendum – New LCD Component section above) cannot be up/downgraded using the image files supplied on v12.40.2 or earlier media. Contact nCipher Support for more information.

4.5. FIPS approved firmware and nShield Connect image

In the event that you wish to use Security World v12.40 with FIPS Approved firmware the latest FIPS approved firmware is provided on the installation media and can be used with the nShield HSMs as given in Table 2.

Table 2 details the directory location of the nShield firmware on the installation media, firmware and image file (for nShield Connect HSMs) and the firmware versions supplied on the installation media.

If the HSM is not supported on the specific operating system the firmware will not be present.

HSM	Directory location on the install media	VSN	Rollback possible?	Firmware version, FIPS status
nShield Connect nShield Connect+	nethsm-firmware/12.40.2cam1-fips/nCx3N.nff	29	N	2.61.2, FIPS certified
nShield Connect XC	nethsm-firmware/12.40.2cam1-fips/nCx3N.nff	29	N	3.4.1, FIPS certified
nShield Solo nShield Solo+	Monitor: firmware/2-60-1/ldb_ncx3p-26.nff	26	Y	-
	Firmware: firmware/2-61-2/ncx3p26.nff			2.61.2, FIPS certified
nShield Edge	Monitor: firmware/2-50-16/ldb_ncx1z24.nff	26	Y	-
	Firmware: firmware/2-61-1/ncx1z26.nff			2.61.1, FIPS certified
nShield Solo XC	firmware/3.4.1/ncx5e-36.nff	36	Y	3.4.1, FIPS certified

Table 2: FIPS Approved firmware and image files provided on v12.40 install media

4.6. Upgrading Solo XC Firmware

If the Solo XC HSM has the earlier 3.3.10 firmware it cannot be upgraded directly to the latest firmware and needs to be first upgraded to an intermediate firmware first. Please contact support and request the firmware upgrade patch from 3.3.10 to 3.3.20. After installing 3.3.20 you will then be able to upgrade to the firmware provided with this release.

5. Compatibility

5.1. Supported hardware

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

- nShield Solo XC
- nShield Solo PCI Express (10+, 500, 6000, 500+, and 6000+)
- nShield Connect (500, 1500, 6000, 500+, 1500+, and 6000+)
- nShield Connect XC
- nShield Edge
- nToken PCI Express "+" (NC2023E-000)
- nToken PCI Express (NC2021E-000): Microsoft Windows, Linux, and Solaris only

5.2. Supported operating systems

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

Operating System	Solo & Solo+	Solo XC	Connect & Connect+ & Connect XC	Edge
Microsoft Windows Server 2016 Nano x64	Y	Y	Y	N
Microsoft Windows Server 2016 x64	Y	Y	Y	Y
Microsoft Windows Server 2012 R2 x64	Y	Y	Y	Y
Microsoft Windows Server 2008 R2 x64	Y	Y	Y	Y
Microsoft Windows 7 x64	Y	Y	Y	Y
Microsoft Windows 10 x64	Y	Y	Y	Y
Red Hat Enterprise Linux AS/ES 6 x86, x64	Y	Y(x64)	Y	Y
Red Hat Enterprise Linux AS/ES 7 x64	Y	Y	Y	Y
SUSE Enterprise Linux 11 x64 SP2	Y	Y	Y	Y
SUSE Enterprise Linux 12 x64	Y	Y	Y	Y
Oracle Enterprise Linux 6.8 x64	Y	Y	Y	Y
Oracle Enterprise Linux 7.1 x64	Y	Y	Y	Y
Linux AS/ES 5 x64 (libc6.5)	N	N	Y	N
Oracle Solaris 11 (SPARC)	Y	Y	Y	N

Operating System	Solo & Solo+	Solo XC	Connect & Connect+ & Connect XC	Edge
Oracle Solaris 11 (x64)	Y	Y	Y	N
IBM AIX 7.1 (Power 8)	N	N	Y	N
IBM AIX 7.1 (Power 6)	Y	N	Y	N
HPUX 11iv3	Y	N	Y	N

Security World v12.40 is only supported on Linux on x86/x64 architectures. Additional main stream x86/x64 based Linux distributions other than those listed above may be compatible, however nCipher cannot guarantee this compatibility.

5.2.1. Supported Virtual environments

The table below shows the virtual environments that are currently supported:

Operating System	Solo & Solo+	Solo XC	Connect & Connect+ & Connect XC	Edge
Microsoft Hyper-V Server 2012	N	N	Y	N
Microsoft Hyper-V Server 2016	N	Y	Y	N
VMWare ESXi 6.5	N	Y	Y	N
Citrix XenServer 6.5	N	Y	Y	N
AIX LPAR	N	N	Y	N

5.3. Strict FIPS 140-2 Level 3 mode – change in behaviour for XC HSMs

This section is reproduced from the earlier s12.20.51 release notes for convenience. The changes in Strict

FIPS 140-2 Level 3 mode continues to apply in v12.40.x releases affecting Solo XC and Con nect XC HSMs (based on 3.4.1 firmware). Please note that this change in behaviour will also be implemented in future Solo+, Connect+ and nShield Edge FIPS certified firmware releases to comply with SP800-131A Revision 1.

Note that an nShield Solo XC or Connect XC (with 3.4.1 firmware) deployed in the same

strict-FIPS Security World as existing Solo + or Connect + HSMs will be constrained by the restrictions detailed below.

Strict FIPS 140-2 level 3 mode is available to constrain the use of algorithms, key sizes and operations to those specified in NIST SP800-131A Revision 1. This mode is available for customers who seek to comply with FIPS 140-2 standard. All security worlds created in strict FIPS 140-2 mode with this release will be compliant to NIST SP800-131A Revision 1.

In addition, please refer to the relevant Security Policy document published on the NIST website for each firmware FIPS certificate. The Security Policy document outlines which algorithms are allowed in strict FIPS mode. Any algorithm not listed e.g. when using custom curves such as Brainpool curves cannot be used in strict FIPS mode. When creating a Security World selecting the *--strict-fips-140-2-level-3* option enforces these restrictions.

In support of strict FIPS 140 mode key generation is blocked for the following key sizes:

	Blocked Key Generation	**Permitted Legacy Support**
1	Triple-DES CBC/ECB 2 keys generation (Triple-DES CBC/ECB 3 key generation is still allowed)	Decryption of ciphertext encrypted with legacy Triple-DES CBC/ECB 2 keys continues to be supported
2	RSA 1024 bit key pairs (Keys must be ⇒ 2048 bits)	Verification of <2048 bit legacy signings continues to be supported. [1]
3	DSA 1024 bit key pairs (Keys must be ⇒ 2048 bits)	Verification of <2048 bit legacy signings continues to be supported. [1]
4	ECDSA P-192, K-163, B-163 (Keys must be ⇒ 224 bits)	Verification of <224 bit legacy signings continues to be supported. [1]
5	DH 1024 bit key pairs (Keys must be ⇒ 2048 bits)	Verification of <2048 bit legacy signings continues to be supported. [1]
6	ECDH P-192, K-163, B-163 (Keys must be ⇒ 224 bits)	Verification of <224 bit legacy signings continues to be supported. [1]

Note [1]: The use of legacy Signing keys (in a legacy Security World) using key sizes disallowed in SP800-131A Revision 1 for further signing operations will invalidate strict FIPS mode.

5.4. Supported compilers for Microsoft Windows C developers

Security World v12.40 C libraries for Windows, built using Visual Studio 2013, have been compiled with the

SDL flag. This makes them incompatible with older versions of Visual Studio (i.e. 2010 and earlier). Microsoft Windows developers using CipherTools or CodeSafe should upgrade to Visual Studio 2013. This applies primarily to static libraries.

5.5. HSM firmware compatibility

A Security World release is only tested with the most recent version of FIPS certified firmware together with the latest firmware release if one exists.

For details on the range of nShield products, latest firmware version, which firmware was shipped with which versions of Security World, and latest FIPS certified version and associated NIST certificate numbers (where applicable) please contact nCipher Support.

5.6. CodeSafe

5.6.1. Supported Development Platforms

In Security World v12.40, CodeSafe development is only supported on:

- Microsoft Windows (Client and Server editions; except for Nano edition)
- Red Hat Enterprise Linux
- SUSE Enterprise Linux

Development for CodeSafe on the other platforms has been removed. Note that CodeSafe applications can be deployed on any supported OS.

5.6.2. nShield XC Compatibility

The CodeSafe runtime on the nShield XC HSMs provides improved efficiency and significantly greater performance and memory, while maintaining a high degree of backwards compatibility.

CodeSafe Applications, or SEEMachines, built against the SEElib API should be source code compatible with the new environment. However they will have to be rebuilt for nShield XC

HSMs. New Makefiles are supplied with the CodeSafe SDK sample code and can be used as a guide for porting.

CodeSafe Applications built against the BSDLib API should be source code compatible with the new runtime environment on nShield XC HSMs. They will have to be rebuilt against the glibsee API. See the Makefileexamples file within the glibsee examples directory in the Code Safe SDK for guidance on the new build parameters; and see the CodeSafe Developer Guide and the API documentation for information on any API changes.

5.6.3. Cross Compiler Update

With the introduction of support for CodeSafe on the nShield XC HSM, a new cross compiler was added (powerpc-codesafe-linux-gnu). This cross compiler replaces the previous cross compiler that was provided for the Solo HSM and should be used for all target platforms.

6. Bug fixes

6.1. Bug fixes host-side

The following table lists the host-side bugs fixed in v12.40:

Bug reference	Description
NSE-11352	Solo XC performance issue on Linux OS platforms affecting symmetric and asymmetric performance has been fixed in v12.40.2 that had regressed in v12.40.0 and v12.40.1
NSE-9584	Removing a physical card from the slot could cause PKCS#11 applications to crash. This has been corrected.
NSE-9437	When retrieving information via SNMP about KeyGeneratingESN from the KeyAdminTable the system would erroneously return 'No Data Available'. This has now been corrected so that the correct information is returned.
NSE-9428	In v12.30 temporary keys created during PKCS#11 key generation were not deleted from the module, potentially causing the module to run out of memory. This has been corrected.
NSE-9314	The conversion of the HP-UX PCI driver to be a dynamically loaded driver in v12.30 introduced an issue whereby the driver installation would fail if that HP-UX system had never had the static PCI driver installed. This issue has been resolved.

Bug reference	Description
NSE-9289	Key generation was not thread-safe when the CKNFAST_ASSUME_SINGLE_PROCESS environment variable was explicitly set to 0 (or N). The code intended to find keys generated by other processes could find a key created by another thread in the same process, before it had been properly recorded in the process's internal records. This would confuse the records and result in some keys not being found. This problem has been corrected by expanding the scope of the lock used to protect the internal structures when CKNFAST_ASSUME_SINGLE_PROCESS is set to 0.
NSE-9276	In Security Wold v12.30 the behaviour of the CKNFAST_ASSUME_SINGLE_PROCESS variable changed, such that setting it to "off" would have no effect. This change has been reverted.
NSE-9205	Under rare circumstances an uninitialised nCore M_Reply structure could be freed, sometimes causing a crash. Every reply structure is now initialised when the command is submitted.
NSE-8854	When the PKCS#11 mechanism CKM_WRAP_RSA_CRT_COMPONENTS was used with an underlying block cipher mode with a block size greater than 64 bits, and also included padding, the mechanism would fail. This has now been corrected.
NSE-8824	The implementation of the AESKeyUnwrap mechanism would fail with an error if the target keytype was a wrapped keytype. This has been corrected so that the mechanism will now succeed.
NSE-8702	If a key is generated in POOL HSM mode then nfkmverify tool fails with the error message "unlimited make recovery blob permission". This error is related to nfkmverify tool and the key usage is not impaired.
NSE-8656	When the nShield SNMP agent was uninstalled from a Windows system the service entry was not removed leaving behind a false entry. This has been corrected so that the service entry is now removed when the SNMP agent is uninstalled.
NSE-8428	With autopush configured, enabling 'UI Lockout with OCS' from the Connect front panel did not update the config on the RFS. The lockout_mode in the RFS config file is now updated correctly.
NSE-7993	Our JCE provider always used the first module for key generation and loading public keys. This has been changed to the first usable module - if the first module becomes unavailable another will be used. In the case of key generation this could potentially affect the OCS used to protect the key. If OCS protection is desired, customers are advised to only use cards from a single OCS in the modules used by JCE.

Bug reference	Description
NSE-7748	Fixed a deadlock that could occur when multiple threads called getinfo or makeacl from nfpython concurrently.
NSE-7462	On a Windows system when retrieving information via SNMP the system.sysDesc value was not being set correctly and would return a value of 'unknown'. This has been corrected so that the correct information is now returned.
NSE-7454	Our JCE provider would only load public keys on the first available module, so that the use of public keys did not benefit from load sharing. Public keys are now loaded on all available modules. The kmjava interface adds support for loading a public key on a list of modules, and for merg ing public keys.
NSE-6800	Installation of Remote Administration Client Tools on Asian versions of Microsoft Windows OS will now complete without error.
NSE-4032	Fixed a bug in the NFKM library which could cause a use limit to be omitted if random num-ber generation failed but world or key creation otherwise succeeded.
NSE-3312	This Remote Administration on the Microsoft Windows Security World ISO now supports the Microsoft Server 2012R2 Operating System. The operating system needs to be restarted after installation.
NSE-3132	When generating a DSA Domain, the PKCS#11 library would erroneously set the pairwise check flag on the nCore command. This flag is no longer set when creating any Domains or Secret Keys. The flag is still set for asymmetric keypair generation.
NSE-2966	The Hardserver previously ran without reporting an error when nt_pipe_users or nt_privpipe_users config entries for restricting client connections contained unsupported syntax, such as a Domain-qualified user or group. The Hardserver service will now refuse to start if there are errors in the config file in order to fail-safe. User and group connection restrictions are supported only unqualified (e.g. to restrict privileged Hardserver connec-tions to a user "alice" who is a domain user, on a machine that is a member of that domain, simply specify the unqualified user name "alice" in the config file for nt_privpipe_users).
NSE-2386	Authentication of the operator card didn’t indicate when the card might have come from another Security World. This indication has now been added.
NSE-2355	oslpy was missing from the AIX distribution, causing the CodeSafe example "mk-preparsed-cert.py" to fail. oslpy is now included.
NSE-1837	The nfdiag diagnostic tool’s log file has been renamed to avoid false-positives from e-mail virus scanners.

Bug reference	Description
NSE-1718	Improved the logging of certain error cases in the Windows PCI driver. NSE-1613 Modified the CNG Wizard application not to set "Prompt always" flag when user selected "Module protection" for OCS. They were able to set at the same time, which was causing some tricky behaviour on our CNG provider.
NSE-1470	Addressed issues that prevented the "csee" example programs from building.
NSE-1410	Fixed CNG provider to select module or card set protection when it need to raise popup, respecting the result that user already decided on CNG wizard.
NSE-298	The Windows USB driver for the nShield Edge has been updated from 2.02.04 to version 2.12.24.
NSE-79	If a PKCS#11 session was incorrectly used by two or more threads at the same time a deadlock could occur. The lock handling has been revised to avoid deadlock, but this is still an application error and should be avoided.

Table 3: Details of bug fixes incorporated into v12.40 host-side

6.2. Bug fixes, nShield Connect & Connect XC image file

Bug reference	Description
NSE-11352	Connect XC performance issue affecting symmetric and asymmetric performance has been fixed in v12.40.2 that had regressed in v12.40.0 and v12.40.1
NSE-8632	If Remote Operator was used via the nShield Connect front panel to import a slot, an error was generated if an attempt was made to subsequently delete the slot. The slot can now be deleted successfully under these circumstances.
NSE-6952	In the v12.10 nShield Connect firmware image, the appliance's secondary network interface is disabled by default; the installer does not check if the interface was enabled, it gets disabled regardless. This is now fixed. If the nethsm_eth1_enable section is missing in the config and the eth1 interface has an IP address configured, the eth1 interface is enabled by default. Newer Connect images would be unaffected by this change as they would have the nethsm_eth1_enable section which would be by default switched off.
NSE-4563	If an nShield Connect has an exported slot configured, when attempting to remove this slot you are able to cancel out of the process before committing. Fixed an issue where cancelling caused an error message to be displayed.

Bug reference	Description
NSE-3940	When retrieving information via SNMP from a system that had multiple nShield Connects, in which one of them was unresponsive, the system might fail to populate many of the netHSM SNMP values for Connects that could be contacted. This has been corrected so that information is now correctly returned from those Connects that are responding.
NSE-11177	Fixed an issue which prevented Connect client licences from being installed on the nShield Connect. The installation would fail with UnknownMechanism. _Note: this issue affected v12.40.0 only and not previous releases. _

Table 4: Details of bug fixes incorporated into v12.40 Connect & Connect XC image

6.3. Bug fixes, nShield XC functionality

The following table lists the bugs fixed in v12.40 that were bugs in the s12.20.00, s12.20.50 and/or s12.20.51 special releases that first introduced the nShield XC product:

Bug reference	Description
NSE-11352	XC performance issue has been fixed in 12.40.2 that had regressed in 12.40.0 and 12.40.1
NGSOL-2844	Connect XC units can enter a failure state with “HSM Failed” displayed on the front panel. The Connect XC fully recovers when power cycled.
NSE-11314	CodeSafe: Mismatched XC CodeSafe headers cause nCore commands to fail in SEE machines. Affects nShield Solo XC and Connect XC and versions v12.40.0 and 12.40.1
NGSOL-2743	RTC value is now persistent after powercycle
NGSOL-2655	The security world information is now cleared when the firmware is upgraded.
NGSOL-2736	Throttled key derivation operations according to product performance variant activation.
NGSOL-2763	CodeSafe example see-enquiry has "Version not understood" errors
NGSOL-2757	SNMP trap generation failing when close to max module memory usage
NGSOL-2751	KML updates for compliance with FIPS186-4
NGSOL-2149	CodeSafe: BufferFull error for messages from SEEMachine to firmware that are close to the max valid length of 256K
NGSOL-2487	CodeSafe: corrected failure to delete file from NVRAM
NGSOL-2723	CodeSafe: updated prebuilt NVRAM user data example sar file
NSE8427/NGSOL2690	Command Generate Random may result in SOS HRM

Bug reference	Description
NGSOL-2564	The library libnfhwcrhk.a for CodeSafe applications was not built correctly due to incorrect endianness. This impacted OpenSSL CHIL functionality.
NGSOL-2721	Reconciled different SOS code reported by the status LED (SOS-HS), and enquiry's 'hardware status' field (SOS-HRS). LED needs to be corrected to report HRS.
NGSOL-2771	Do not apply Solo XC configuration flags when a software update has failed.
NGSOL-2799	Resolve Solo XC detection issues with Fujitsu M10-1 Solaris Sparc server
NGSOL-2792	CodeSafe: corrected timeout for the select() calls. Now it times out as per the timeout value specified in the select() parameters.
NGSOL-2789	Updated key derivation throttling coefficients to consider latest Solo XC performance. Improvement to NGSOL-2736.
NGSOL-2770	Patches for eglibc vulnerabilities CVE-2015-8982 & CVE-2015-8983
NGSOL-2762	Addition of the EMV feature in Solo XC for SafeSign.
NGSOL-2758	Patch for integer overflow vulnerability in Shadow package - CVE-2016-6252
NGSOL-2759	Added AIS-31 to Solo XC
NGSOL-2797	Fixed SOS-HRS seen while running test_interactive.py

Table 5: Details of bug fixes incorporated into v12.40 nShield XC functionality (includes specific host-side XC functionality, Connect XC and Solo XC fixes)

7. Security World v12.40 known issues

7.1. Known issues, host-side

Defect Reference	Description
NSE-6195	Attempting to install a warrant on a SoloXC in pre-maintenance mode returns with an incorrect error. The workaround is to install the warrant while the module is in operational mode.

Defect Reference	Description
NGSOL-2606	The csddoc directory with HTML documentation for the nCore/NFKM APIs inside the module is not installed along with the CodeSafe Developer Toolkit. The directory can be found in the document directory on the installation media. If desired, the user may copy the directory to the document directory under the software installation point, and be prepared to manually remove it upon uninstallation of the CodeSafe Developer Toolkit.
NSE-9230	The installer on Windows often gives a prompt to find setup.exe during installation. Click 'OK' at the prompt to accept the default location and installation completes successfully.
NSE-12118	A regression in v12.40.2 results in nTokens with part number NC2021E-000, identifiable as those without a blue nCipher heatsink, not being detected automatically by the hardserver. Prior to v12.40.2 nTokens would appear automatically in the hardserver's enquiry output. As a work-around, set serial_dtpp_devices=COM7 (or whatever COM port) in the hardserver server_startup section. Note some trial and error may be required as the nToken actually uses two COM ports, and only one is provided to the hardserver. If the wrong port is specified, it will appear as Failed in enquiry.

Table 6: Known issues in v12.40 host-side software

7.2. Known issues, nShield XC functionality

The following tables lists the known issues with the nShield XC (Solo XC and Connect XC)

Defect reference	Description
NGSOL-2494	Remote mode change does not work from a virtual machine that imports the nShield Solo XC board. Remote mode change should be done on the VM that directly communicates with nShield Solo XC board.
NGSOL-2551	Interrupting the "new-world –program" command may require the nShield Solo XC board to be power cycled.

Defect reference	Description
NGSOL-2744	If a Solo XC is powered up and the power supply is then removed within 20 seconds the unit may enter a state where the internal back-up battery is being discharged at a higher rate than normal. Similarly, if a Connect XC is powered up and the mains supply is then removed (via the rear rocker switches or removing both mains cables) within 20 seconds the unit may enter a state where the internal back-up battery is being discharged at a higher rate than normal. If left in this condition for an extended period, the Solo XC /Connect XC will enter a failed state, indicated by an SOS-B morse error code on the status LED. To avoid this occurrence, should a Solo XC or Connect XC be turned off under such conditions, power should be reap plied as soon as possible and the unit left powered until it has successfully booted into an operational mode. Note that some electrical safety tests such as leakage current testing may create these con ditions, so it is recommended that the unit is booted into an operational mode after any safety testing, as described above. Note: This will not affect Connect XC units with serial number 36-XC0384 and above and Solo XC units with serial number 36-X00527 and above. This issue will be fixed for any units within the affected range in a forthcoming release.
NSE-10137	When upgrading the Solo XC firmware if there is a security processor update then the VM host needs to be rebooted. It is not sufficient to just reboot the VM.
NSE-11669	Solo XC/ Connect XC enquiry output reports incorrect HSM product code. Presently reports: product name nC3025E/nC4035E/nC4035N. Should be product name nC3025E/nC4035E/nC4335N as stated in the FIPS certificates.

Table 7: Known issues in nShield XC functionality

7.3. Known issues, interoperability

Defect reference	Description
NSE-7618	When an SEE (restricted) feature certificate is applied at the front panel of the Connect, it will apply successfully, but will not be reported when running the feature enable tool *fet* on a client of the Connect.

Table 8: Known issues in interoperability in v12.40

7.4. Known issues, firmware / image file up/downgrading

Defect reference	Description
NSE-10779	It is not possible to downgrade a v12.40.x non-FIPS nShield Connect+ image file (containing non-FIPS firmware) to an image file containing FIPS certified firmware, despite the upgrade appearing successful. The nShield Connect image file Version Security Number (VSN) is the same for both FIPS and nonFIPS - VSN36) enabling a downgrade. However v12.40.x non-FIPS firmware (VSN 29) is higher than the 12.40.x FIPS firmware (VSN 28) and this prevents a successful downgrade to the FIPS firmware. There is presently no work around for this issue. This does not affect upgrades to v12.40.x from v12.30 or earlier Connect+ images. This issue does not affect nShield Connect XC units.
NSE-5662	nShield Connect can occasional get stuck in POST when powering on, performing a reboot or initiating a front panel/remote upgrade. Work around is to power off/power on nShield Connect using the PSU rocker switches. Note a remote reboot using the netHSMadmin utility will not resolve this issue.

Table 9: Known issues, firmware /image file

8. Known issues from earlier Security World releases

Known issues from releases prior to Security World v12.40 include the following:

8.1. Security World

Bug reference	Description
NSE-11886	CNG Wizard does not allow the creation of a Security World when a nToken is present, as this requires the operator to put all the modules into "Initialisation Mode".
NSE-11885	Hardserver ignores settings for nt_pipe_users if Java ports are open
NSE-11911	Solo and Solo+ behave differently to the SoloXC when restarting the hardserver in premaintenance mode. When clearing the modules while in pre-maintenance using \{\{nopclearfail c -m1}} they all (Solo, Solo+ and SoloXC) return to operational mode.
NSE-8463	When enrolling an nShield Connect into a security world or creating a new security world you must ensure that the world and module files are propagated to client machines and afterwards ensure that hsc_configurepoolmodule -mN is run on each machine enrolled as a client where N is the newly enrolled module number.

Bug reference	Description
NSE-7575	The user won't see the max exported modules being updated when running enquiry after remotely enabling the client licences dynamic feature due to the enquiry cache not being cleared for imported modules. User should restart the client-side hardserver to work around this issue.
NSE-7456	The nShield PKCS#11 client library can only read FIPS Authorization from operator cards, not from Administrator Cards. When used with a Strict FIPS 140-2 Level 3 compliant Security World, an Operator Card Set must be created for the PKCS#11 to be able to present FIPS Authorization to the module(s).
NSE-7025	The nShield Remote Administration Client is not supported on SLES 11.
NSE-6391	On Solaris systems, the system path /usr/sbin must be in the PATH environment variable when executing /opt/nfast/sbin/install and /opt/nfast/sbin/init.d-ncipher. Suggested usage: PATH=/usr/bin:/usr/sbin /opt/nfast/sbin/install
NSE-6610	Security World applications which write to log files lock the log files when writing log messages. This includes the hardserver when writing to /opt/nfast/log/hardserver.log. If another application, such as a backup application, holds a lock on the log file for an extended period, the Security World application will be blocked for that time. It is recommended that either log files should not be locked whilst applications are running, or that they be locked only briefly whilst copying the file.
NSE-3827	The pathname of Codesafe executable files should only contain ASCII characters. If non-ASCII characters are included in the pathname StatusMalformed will be returned when a connection is made through the Generic Stub.
NSE-2115	Log files produced by the Security World software on 32-bit Linux systems are limited to 2 GB. This includes the hardserver log in /opt/nfast/log/hardserver.log. Applications, such as the hardserver, will not start if their log files exceed this size. The user should delete log files periodically (backing up first if required) to avoid this problem. This issues does not affect 64-bit Linux systems.
NSE-4099	**Windows Platforms Only** If nShield logging is enabled, the file specified by NFLOG_FILE must be writable by the user running the 'nShield Service Agent' or the agent will not be able to process dialogs from a CNG service in Session 0.
NSE-4094	**Windows Platforms Only** Having run the CNG installation wizard or cngregister, it is necessary to log off and log in to start the nShield Service Agent. The Agent can be started explicitly by executing either nShieldServiceagent.exe or nShieldServiceAgent64.exe from the %NFAST_HOME%\bin folder.
MEI-4046	nShield Solo is not supported in AIX Power8 hardware Architecture
NSE-2671	Codesafe SEELib "nvram" example SEE machine crashes on startup.

Bug reference	Description
NSE-1361	Microsoft Windows: Set path before running "HTTPSD with client authentication" example Under Microsoft Windows ensure that %NFAST_HOME%\bin has been added to the system PATH environment variable before running the CodeSafe example "HTTPSD with client authentication"
NSE-2899	CNG Wizard says "There was an error reading the card" when it means "card not in Authorized Card List".
MEI-4304	nfwarrant claims the module is in pre-initialization mode if the module is uninitialized. Switch to Initialization mode and run initunit, then put the module back in Operational mode, before running nfwarrant.
MEI-4249	The Remote Administration Service does not abort associations when a dynamic slot is unavailable due to CrossModule#NetworkError. Break and remake the association from the Remote Administration Client.
MEI-4463	Applications that call NFKM_checkconsistency display "nfkmcheck: warning: World kmdata entry E0x199=E409 unexpected"
MEI-4386	The [slot_imports] and [slot_exports] sections of the hardserver config file is misleading in stating "This cannot be configured alongside dynamic slots." The restriction is dynamic slots cannot be exported hence cannot be imported.
MEI-4306	Connect UI login using OCS displays UnlistedCard for Remote Administration smart cards if card is already inserted. Removing and reinserting the card is required.
MEI-3934	Running enquiry on an nShield Edge results in hardware status being reported as "unsupported driver." This is normal behaviour; SOS error reporting is not available on an nShield Edge.
NSE-2857	Failed to start nFast service error message seen occasionally after installing on Windows. If services are running error can be ignored.
MEI-4569	Display World Info on nShield Connect front panel may show a valid Remote Administration smart card as 'Unidentified'. Use *slotinfo* to confirm smart card is valid.
MEI-2149 /NSE-3426	nShield Connect front panel UI appears to run slow after a Connect image upgrade. The workaround is to reboot the Connect after the upgrade after which the front panel will behave correctly.
MEI-4587	If the environment variables NFAST_SERVER_PORT and NFAST_SERVER_PRIVPORT are set to non-standard values, e.g. 9100 and 9101 respectively then the Remote Administration Service will not start.
MEI-4559	'nethsmadmin –-reboot' option does not time out or return when a module has been marked as failed. You should check your Windows event viewer to check for time outs and then terminate the 'nethsmadmin' application.
MEI-4572	Generatekey ignores slot choices and will use an OCS in any available slot of the chosen module.

Bug reference	Description
MEI-4586	The nShield Connect can sometimes hang on start up after performing a tamper. Please contact Support for further information on this issue.
15318	It is not possible to recover PKCS #11 keys using the nShield Connect or netHSM unit's front panel. You must use the rocs client-side utility to do this.
MEI-3265	When upgrading from any previous installation the hardserver configuration file will not be populated with the new remote administration sections, resulting in default behaviours. A new default configuration file can be made by running "cfg-mkdefault -r", remember to back up your existing configuration file before running this operation.
MEI-4418	When creating a Security World on a Windows client host, the new-world utility can fail with TokenMessageError until the module is cleared. If this happens, clear the module (using nop clearfail -c, the clear button on the Edge or the Solo Board, or the menu command on the Connect) before re-attempting to create a Security World.

Table 10: Known issues with v12.30

8.2. Remote Administration Client v1.10

Bug reference	Description
NSE-11849	Hardware error reporting and MOI changes do not work in HPUX
MEI-3390	When using Ubuntu 12.04 and later then the jpeg compatibility library package libjpeg62 must be installed for the Remote Administration Client.
NSE-2861	Multiple Remote Administration GUI clients on a PC can use the same card reader to connect to multiple dynamic slots, causing one or both to work incorrectly, eg reporting UnknownCard. Avoid doing this.
MEI-2801 MEI-2805	You are recommended to not use more than four TVDs or standard card readers on a single Remote Administration Client system as it can run out of resources if an excessive number of card readers are used.
NSE-2853	RHEL 7 Smart Card Manager can cause Unknown Card due to Sharing Violation; the smart card manager needs to be turned off to prevent the sharing violation.
MEI-2481	RSA token card services prevent the Remote Administration Client from working on Microsoft Windows OS (e.g. RAC hangs displaying "reading..."); these need to be disabled in the Windows Task Manager services table to allow Remote Administration smart cards to work with both the TVD and other smart card readers.
MEI-4480	On rare occasions, leaving a Remote Administration smart card in a dynamic slot for a prolonged period can result in SecureChannelFailed.

Bug reference	Description
MEI-4412	Using the Remote Administration Client on the same machine as Microsoft ADCS may result in the smart card service crashing, causing the RAC to fail.
NSE-2860	Switching to Maintenance mode while an Association with a dynamic slot exists causes an UnknownCommand error
MEI-3940	Remote Administration Support Client Tools Setup can pause for up to 2 minutes with no feedback to user (Windows)
MEI-4029	Running racgui on SUSE 12 shows GTK assertions from wxpy
MEI-4401 MEI-3383	Any previous nShield Security World Software must be uninstalled before installing the Remote Administration Client software. If you want the Remote Administration Client software installed alongside your Security World Software it is available (and installed by default) via the Security World Software installer.
NSE-6939	On OS-X the Tab key does not navigate between controls on the wizard pages and the Return key does not perform the default action. All operations can be accomplished with either a mouse or touchpad.
NSE-7088	Installing the RAC on OS X for the current user will not recognize the TVD. This is due to the TVD driver not being installed in this scenario. It is necessary to install separately the TVD driver for all users to allow the TVD to be recognized.
MEI-4557	Occasionally TokenSecureChannelError reported when creating/loading a security world using a Remote Administration smart card. Remove and re-insert the card.

Table 11: Known issues with v1.10 Remote Administration Client

9. Security World Remote Administration

9.1. Remote Administration

Gathering a quorum of card holders to carry out card holder duties in a remote datacenter can be expensive and inconvenient. The Remote Administration feature introduced in Security World v12.00 enables Administrators and Operators to present their cards remotely to authorise HSM operations without being physically present at the HSM. This enhanced functionality is achieved by extending the existing Security World architecture to support a secure channel to a remote application running on a smart card.

Prior to the introduction of Remote Administration, Administrators were able to perform limited HSM administration operations using their preferred remote access solution (eg. Secure Shell (SSH), Remote Desktop etc). Remote Administration requires Administrators to use their remote access solution to perform these administration operations and extends

the operations that can be performed in this way.

Remote Administration enables:

- card holders to present smart cards to an HSM that is in a different location (e.g. the card holder may be in an office, while the HSM is in a datacenter)
- all Administrator and Operator card operations to be carried out in a different location from the HSM, including use of non-persistent Operator Cards Sets
- Security World programs and utilities to be run remotely, when used in combination with a standard remote access solution
- full remote administration of Security Worlds and their HSMs including:
  - Remote mode change
  - Create/load/unload Security World
  - Remote firmware upgrade of nShield Connect and nShield Solo firmware (after upgrade to v12.00)
  - Module status (SOS) reporting
  - nShield Connect reboot
  - nShield Connect front panel lock out

9.2. New components

Remote Administration involves a number of new and replacement components:

9.2.1. nShield Remote Administration smart cards

New nShield Remote Administration smart cards are needed for Remote Administration. The cards provide:

- storage and retrieval of logical token fragments, similar to the smart cards used with previous releases
- security mechanisms to ensure authentication and confidentiality of data transferred between itself and the HSM

The nShield Remote Administration smart cards are designed to be FIPS 140-2 Level 3 certi fied devices, supporting execution of a custom Java Applet developed by nCipher Security. The smart cards used with previous versions of Security World software and nShield HSMs are still useable with v12.00 but, as previously, only in an HSM's local slot. Remote Administration smart cards can be used both remotely and in an HSM's local slot.

To use most remote administration features you must use Remote Administration smart

cards. See figure 1 below:

Figure 2: Remote Administration smart cards

Existing Administrator smart cards can be migrated to new Remote Administration smart cards using the *racs*

(replace administrator card set) utility. Similarly existing Operator card sets can be migrated using the *rocs* (replace operator card set) utility, provided the Security World has recovery enabled and the keys protected by that OCS are recovery enabled.

Figure 3: Migrating existing card sets to Remote Administration card sets using rocs or racs

9.2.2. Authorised card list

The use of nShield Remote Administration smart cards, both remotely and in an HSM's local slot, is controlled by an Authorized Card List. If the serial number of a card does not appear in the Authorized Card List, it cannot be used by the system. The list only applies to Remote Administration smart cards.

By default, the Authorized Card List is empty following software installation. The serial num bers of Remote Administration smart cards must be added to the list using a text editor before they can be used.

For more information on the Authorized Card List see Chapter 4 of the nShield Solo User Guide or Chapter 6 of the nShield Connect User Guide.

When administrative operations involving Remote Administration smart cards are initiated from an nShield Connect's front panel, the nShield Connect fetches the Authorized Card List from the RFS.

It is necessary to keep the Authorized Card List in sync by copying the file between the RFS and clients manually.

9.2.3. Remote Administration Client

The Remote Administration Client (RAC) is a utility that enables you to select an HSM located elsewhere from a list provided by the Remote Administration Service (RAS), and associate an nShield Trusted Verification Device attached to your computer with the HSM.

The RAC GUI (usually running on a laptop or workstation) communicates with the RAS (in a datacenter) over a standard TCP/IP connection. If the RAC computer is not on the same local network as the RAS computer, nCipher recommend that the connection is made over a VPN.

Figure 4: Sample screen from the Remote Administration client GUI

In the above example screen, an HSM will not be "Remote Administration (RA) Ready" until it has the appropriate firmware, has a P521 based warrant and has one or more dynamic Slots configured. For users who want to script the card presentation process, there is also a command line utility, *raccmd*.

See the Release Notes for nShield Remote Administration Client v1.0 and the Remote Administration Client User Guide for more information on deploying and using the Remote Administration GUI or command line utility.

9.2.4. Remote Administration Service

The Remote Administration Service (RAS) provides a bridge between the RAC and the back end HSMs (via the hardserver). Its functionality is to:

- manage connections from multiple RACs
- supply a list of available HSMs to the connected RACs
- negotiate a connection to an HSM via the hardserver and route messages between the RAC and destination HSM

When setting up the RAS you need to open port 9005 (default value) in your firewall. Refer to the Firewall settings section of the appropriate nShield Installation Guide for more detail.

The RAS participates as a crypto client of the HSMs. As such, the server used to host this software component must be a licensed client of the nShield Connects being remotely administered. If your Remote File System (RFS) is already a licensed client, the RAS can be

collocated on the RFS server without needing to purchase an additional client license.

9.2.5. nShield Trusted Verification Device (TVD)

nCipher supply and recommend the use of the nShield Trusted Verification Device (TVD). This is an intelligent smart card reader that blocks any malware on the client machine from spoofing the HSM identity passed to the nShield Remote Administration smart card.

Figure 5: nShield Trusted Verification Device (TVD)

9.3. HSM warrant upgrade

nShield Connect HSMs have a P521 elliptic curve based warrant (also known as a KLF2 warrant) created during the manufacturing process. No in-field warrant upgrade is necessary for nShield Connects.

nShield Solo and nShield Edge HSMs are factory warranted with a 1024-bit DSA key which is not a suitable root of trust for Remote Administration. An in-field warrant upgrade to a P521 elliptic curve based DSA key is necessary to use any nShield Solo or nShield Edge with Remote Administration smart cards.

If you are planning to use Remote Administration smart cards with an nShield Solo or nShield Edge, you need to initiate a Certificate Signing Request (CSR) to send to nCipher Support to generate a P521 EC based warrant.

To generate a CSR, run the command line tool *nfwarrant --csr --req <module>*. This creates a text file containing public key information which should then be sent via email to nCipher

Support to generate a P521EC based warrant.

nCipher Support will email the warrant back to you. To install the warrrant on your nShield Solo or nShield Edge HSM, run the command line tool *nfwarrant --warrant --install <file>*.

Refer to Appendix B: Warrant Management of the appropriate user guide for further information on warrant upgrade.

9.4. HSM configuration

To support Remote Administration, HSMs have to be configured to support between 1 and 16 Dynamic Slots. The default is zero which disables remote card presentation. These Dynamic Slots are virtual card slots that can be associated with a card reader connected to a remote computer. Dynamic Slots are in addition to the local slot of an HSM and any soft token slot that may be available.

Use the *dynamic_slots* section in the client configuration file to define the number of Dynamic Slots for each relevant HSM, see **New configuration file sections** below and refer to the nShield Solo and nShield Connect User Guides for more information on client configuration files and how to configure Dynamic Slots.

Alternatively nShield Connect Dynamic Slots can be configured via the front panel controls by navigating to **Security World mgmt** > **Set up dynamic slots** > **Dynamic slots**.

9.5. Further details

9.5.1. New nethsmadmin tool

Security World v12.00 introduced a new tool to provide Remote Administration capability for an nShield Connect without accessing the front panel.

Options include:

- Checking the Security World files on a specified nShield Connect
- Copying Security World files from the RFS to the nShield Connect
- Commanding the specified nShield Connect to reboot
- Commanding the nShield Connect to upgrade using the specified nShield Connect image file from its RFS
- Retrieve a list of nShield Connect image files available on the RFS

For more information, see Chapter 6 of the nShield Connect User Guide.

9.5.2. Ability to remotely change the mode of an nShield Solo or nShield Connect

The mode of an nShield Solo HSM (Maintenance/Operational/Initialisation) or an nShield Connect

(Operational/Initialisation) can be changed remotely using *nopclearfail*. For more information, for nShield Solo see the nShield Solo User Guide, **Appendix: Checking and changing the mode**, and for nShield Connect see the nShield Connect User Guide, **Appendix: Checking and changing the mode**.

Remote mode switching is not available on an nShield Edge.

9.5.3. New jumper switch settings in nShield Solo

A previously unused jumper switch on nShield Solo HSMs provides the ability to enable and disable remote mode changing of a Solo HSM. For more information, see the nShield Solo User Guide, **Appendix: Checking and changing the mode on an nShield Solo module**.

9.5.4. New additions to Enquiry utility

Running an *enquiry* for nShield HSMs now includes the following new entries:

- Image version – this lists the version of image file on an nShield Connect
- Hardware status – Error codes identified by the blue Status LED flashing Morse SOS codes are now also reported in the hardware status field of the enquiry output. During normal operation the Hardware status is reported as 'OK'. SOS error reporting is not available on an nShield Edge

9.5.5. New feature to reformat Operator Cards

It is now possible to reformat and re-use Operator cards using the *slotinfo* command with *ignoreauth* flag, eg *slotinfo -m1 -s2 --format --ignoreauth*. Refer to the appropriate User Guide for more detail. This applies to Remote Administration smart cards only.

9.5.6. New configuration file sections

The following new sections pertinent to Remote Administration have been added to the hardserver configuration file:

9.5.6.1. [server_settings]

```
# Is remote mode changing enabled on this system? (default=yes)
# enable_remote_mode=ENUM
#
# Is remote reboot enabled on this system? (default=yes)
# enable_remote_reboot=ENUM
#
# Is remote upgrade enabled on this system? (default=yes)
# enable_remote_upgrade=ENUM
```

The server_settings section is relevant for nShield Connect only. It does not apply to nShield Solo HSMs.

9.5.6.2. [dynamic_slot_timeouts]

```
# Start of the dynamic_slot_timeouts section
# Timeout values used to specify expected smartcard responsiveness for all
# modules on the network.
# Each entry has the following fields:
#
# Round trip time limit, in seconds, is how long to wait before giving up due
# to network delays. (default=10)
# round_trip_time_limit=INT
#
# Maximum time, in seconds, that can pass without a response from the
# smartcard before considering it removed and unloading all associated secrets
# (default=30)
# card_remove_detect_time_limit=INT
```

The dynamic_slot_timeout section is in the Module configuration file for nShield Connect HSMs and the hardserver configuration file for nShield Solo HSMs.

9.5.6.3. [dynamic_slots]

```
# Start of the dynamic_slots section
# The dynamic smartcard slots that the modules should provide for the use of
# administrators who do not have physical access to the module hardware
# Each entry has the following fields:
#
# ESN of the module to be configured with dynamic slots.
# esn=ESN
#
# Number of dynamic slots the module will support. (default=0)
# slotcount=INT
```

The dynamic_slots section is in the Module configuration file for nShield Connect HSMs and the hardserver configuration file for nShield Solo HSMs.

9.5.6.4. [slot_mapping]

```
# Start of the slot_mapping section
# Slot remapping configuration.
# Each entry has the following fields:
#
# ESN of the module on which slot 0 will be remapped with another.
# esn=ESN
#
# Slot to exchange with slot 0. Setting this value to 0 means do
# nothing.(default=0)
# slot=INT
```

The slot_mapping section is in the Module configuration file for nShield Connect HSMs and the hardserver configuration file for nShield Solo HSMs.

Mapping a Dynamic Slot to slot 0 is needed if you want to use Remote Administration with applications that are not aware of slot numbers greater than zero. This applies to KeySafe and CNG Wizard but may also apply to your own applications.

9.5.6.5. [remote_administration_service_startup]

```
# Start of the remote_administration_service_startup section
# Remote Administration Service communication settings, these are only read at
# Remote Administration Service startup time
# Each entry has the following fields:
#
# The port for the Remote Administration Service to listen on for incoming TCP
# connections from remote administration clients (default=9005)
# port=PORT
```

9.5.6.6. [ui_lockout]

```
# Start of the ui_lockout section
# UI lockout settings
# Each entry has the following fields:
#
# Set to "locked" to enable UI lockout without requiring a logical token. Set
# to "locked_lt" to enable UI lockout with a logical token (requires a valid
# ltui_hash to be set) or "unlocked" for no UI lockout (default=unlocked).
# lockout_mode=ENUM
#
# The hash of the logical token (LTUI) required to authorise access to the
# unit menu structure when the lockout_mode is set to locked_lt; if the
# lockout_mode is locked_lt and a valid hash is provided then the lockout will
# be enabled. Default is all-zero (disabled).
# ltui_hash=HASH
#
# Set to "no" to disable the front panel power switch in Operational mode.
# (default=yes, power switch causes shutdown)
```

```
# panel_poweroff=ENUM
```

The ui_lockout section is relevant for nShield Connect only. It does not apply to nShield Solo or nShield Edge HSMs.

To update an existing hardserver configuration file, edit and insert the sections above. Alternatively factory resetting an nShield Connect will generate a new configuration file including the new Remote Administration relevant sections listed above. See the appropriate User Guide for more information on editing and loading configuration files. See also known issue MEI-3265.