nShield Security World

nShield Security World v12.50.4 Release Notes

4 March 2024

Table of Contents

1. Introduction

These release notes apply to version 12.50.4 of Security World Software, CipherTools, and CodeSafe for the nShield family of Hardware Security Modules (HSMs). They contain information specific to this release such as new features, defect fixes, and known issues.

Security World Software is for users of nShield Solo (PCI Express variants), nShield Connect, and nShield Edge. However, this release is only supported on Microsoft Windows and Linux platforms.

The Release Notes may from time to time be updated with issues that have come to light after this release has been made available. Please check https://nshieldsupport.entrust.com for the most up to date version of this document.

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

1.1. Document History

Revision	Date	Description
1.2	2024-03-04	PDF branding update, including adding this version history table and updating the support contact information. No content changes to product or the Release Notes.
1.1	2019-05-17	Addition of details of the 12.50.4 release.
1.0	2018-10-30	Initial revision of document.

1.2. Purpose of this release

Security World version 12.50 introduces enhancements to version v12.40 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 Security World v12.50.4. If you are using v12.50.1 Preview release you should upgrade unless you are evaluating NTP, see known issue NSE-15822.

2. Security World v12.50.4

Security World v12.50.4 release addresses an issue affecting the nShield Connect image that caused the nShield Connect HSM to become unresponsive when syslog was enabled to send Connect logs and/or Audit logs off the Connect to a syslog server. The occurrence of this issue is dependent upon the load of the HSM and how many log messages are sent. If this issue occurred, restarting the nShield Connect would return it to an operational state. This issue affected all variants of the nShield Connect hardware and both the FIPS and non-FIPS version.

2.1. Changes in v12.50.4

The following changes have been made in the v12.50.4 release:

- Updated nShield Connect images containing a fix for the syslog issue. This image has the version number 12.50.4.
- Updated ISOs for all the 12.50 supported operating systems to contain the updated nShield Connect image. The version number of these ISOs is now 12.50.4.
- Updated installers to contain the updated Connect images. The version number of these installers is now 12.50.4.

2.2. Existing nShield Connect deployment with v12.50.2 installed

If you already have v12.50.2 Security World software installed there is no need to uninstall this and install v12.50.4. There are no changes to the host side software.

The installation installs the Connect images into `%NFAST_HOME%\nethsm-firmware` directory and so a v12.50.2 installation will contain the older connect images. These can be manually updated by copying the Connect images from the ISO into that directory

2.2.1. Installing the updated Connect image

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 Upgrading from previous releases.

2.3. Existing nShield Solo and nShield Edge deployment with v12.50.2 installed

If you already have v12.50.2 Security World software installed there is no need to uninstall this and install v12.50.4. There are no changes to the host side software.

3. Main features of Security World v12.50

This section summarises the main features introduced with Security World v12.50.

3.1. Integrated nShield XC support

The v12.40 release introduced common support for the nShield Solo+, Solo XC, Connect+, and Connect XC HSMs on the same Security World release. However, the features supported across the different HSM variants varied. Security World v12.50 introduces a common baseline of features for all nShield HSM platforms.

The table below shows some of the recent HSM features added and the version of Security World that feature was added.

The features added in v12.50 discussed below are present on all HSMs.

Table 1 Features present in the different nShield HSMs

Feature	Solo/Solo+ Connect/Connect+	Solo XC Connect XC
Remote Administration	v12.00	v12.40
Pool Mode	v12.30	v12.50 (new)
SafeSign Cryptographic Module mechanisms	v12.40	v12.40
Deterministic DSA	v12.40	v12.50 (new)
Derive key support for Hyperledger	v12.40	v12.50 (new)
DeriveKey ACLs	v12.40	v12.50 (new)

3.2. FIPS Certification and required changes

The module firmware has been updated in preparation for recertification against the FIPS 140-2 standard.

If a Security World created on host software prior to v12.50 is loaded onto the updated firmware then there will be no functional change in behaviour. However, if you have a requirement for compliance against FIPS 140-2 level 3 this is not a valid combination and you should continue to use your existing FIPS compliant firmware.

If a new Security World is created on v12.50 host software the functional changes listed below will occur.

Note - A new Security World can only be created in this release using the new-world command. Other methods for creating a Security World have not been updated.

- The default value for UseStrongPrimes will be on in the default Security World
- Only one CipherSuite is supported for creating a new Security World
- Some additional user-selectable cryptographic mechanisms will be restricted in Security Worlds created to be compliant with FIPS 140-2 Level 3. These restrictions are shown in the *Cryptographic Algorithms* appendix of the *User Guide*
- A number of the internal cryptographic mechanisms have been updated to a higher security strength and the previously used mechanisms have been restricted. These internal mechanisms are used in all v12.50 Security Worlds.
- The Diffie-Hellman (DH) key type and associated mechanisms has been replaced by the DHEX key type

The KLF mechanism has been replaced by KLF2, which means that it will not be possible to request a warrant upgrade for a module that is part of a v12.50 Security World. It is recommended that all warrant upgrades are completed prior to upgrading to Security World v12.50. Should a warrant upgrade be needed on a module that is part of a v12.50 Security World it will be necessary to remove the module from the v12.50 Security World, request the warrant upgrade and then re-indoctrinate the module into the v12.50 Security World.

3.3. Audit Logging

Support has been added for users of nShield HSMs in regulated environments where there is a requirement to provably log events. The Audit Logging facility provides the following features:

- Tamper evident logging of relevant nCore command execution on the HSM
- Cryptographic key life cycle traceability
- Authorization for key usage
- Key loading onto HSM
- Optional logging of key usage
- Key destruction
- Compatibility with syslog and SIEM infrastructures
- Logs produced in Common Event Format (CEF)

Audit Logging can only be used on new Security Worlds and is enabled when a Security World is created. For further details see the relevant *User Guide*.

3.4. nShield Connect HSM time synchronisation

A standard NTP client has been added to the nShield Connect HSM to support synchronisation of system time on the Connect with one or more NTP servers. Network Time Protocol (NTP) is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC). System time on the nShield Connect is independent of the Real Time Clock (RTC) in the HSM and is used for log messages and front panel display.

NTP is configured using the new cfg-pushntp utility on a client computer. For further details see the *Connect User Guides*.

3.5. Common Criteria CMTS Mode

Support has been added for creating Security Worlds that meet the requirements of the EN 419 221-5 Protection Profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services.

3.6. Softcard support in nShield CNG Key Storage Provider

Support has been added in the nShield CNG Key Storage Provider for creating and loading private keys protected by Softcards, in addition to the existing module-protection and Operator Card Set protection options that were already available.

If Softcard or Operator Card Set protection is selected in the CNG Configuration Wizard, a specific Softcard or Operator Card Set must also be selected. This differs from the behaviour in previous releases where the Operator Card Set to be used for protection was not specified explicitly in the wizard, and any Operator Card Set that could be auto-loaded might have been used when generating a key.

If it is required that different CNG keys be generated with different protection options, use the "Allow any protection method to be selected in the GUI when generating". This will then cause a key generation wizard to be displayed when generating the key, enabling module protection or protection with any available Softcard or Operator Card Set to be selected.

Note that the CNG Configuration Wizard options for protection affect the generation of new keys, and don’t affect the loading of existing keys, which continue to be loadable even if they were generated with different protection options.

3.7. Operating system support

Support for the Microsoft Windows Server 2016 Core edition has been added.

Microsoft Windows Server 2016 Nano edition is no longer supported. Contact nshield.support@entrust.com if you require further information.

3.8. Additional algorithm support

The X25519 ECDH key exchange function and the Ed25519ph variant of the Ed25519 signature scheme (both based on curve25519) are now supported by nCore and the PKCS#11 library.

The following Brainpool curves are now supported as named curves by nCore and the PKCS#11 library:

`BrainpoolP160r1`, `BrainpoolP160t1`, `BrainpoolP192r1`, `BrainpoolP192t1`, `BrainpoolP224r1`, `BrainpoolP224t1`, `BrainpoolP256r1`, `BrainpoolP256t1`, `BrainpoolP320r1`, `BrainpoolP320t1`, `BrainpoolP384r1`, `BrainpoolP384t1`, `BrainpoolP512r1` and `BrainpoolP512t1`.

3.9. Additional PKCS#11 mechanism support

Support for the `CKM_AES_KEY_WRAP` mechanism has been added to the PKCS#11 library. This was previously only supported by the nCore API.

3.10. nShield Connect can directly send hardserver and system logging to a remote logging service (SIEM)

The nShield Connect hardserver log and system log entries can now be directly sent to a remote syslog or SIEM type service. This can be in addition to, or instead of, sending logs to the RFS.

4. Important notes on Security World v12.50

The following section contains important information that should be noted for this v12.50 release:

4.1. Security World Creation

It is only possible to create a new Security World on v12.50 module firmware with v12.50 host software. An attempt to use v12.50 host software to create a new Security World on older firmware will result in an error, as will an attempt to load a v12.50 Security World onto HSMs operating with older firmware. Key migration from old worlds to the newly created 12.50 security world is not currently supported.

4.2. Security World Types

Security World v12.50 introduces a number of Security World modes, which define how the Security World is set up. The possible modes are:

- Unrestricted (default)
  - This is similar to default non-strictfips worlds created in pre-v12.50 Security Worlds.
- FIPS-140-2-Level-3
  - This is equivalent to strictfips mode in pre-v12.50 Security Worlds. It creates a Security World compliant with FIPS140-2 Level 3.
- Common-Criteria-CMTS
  - Creates a Security World compliant with Common Criteria PP 419 221-5

For this v12.50 release it is recommended that the default unrestricted mode is used. While creating a Security World in one of the other modes is possible, these are still going through certification and so may need to change to be fully compliant. These modes will be fully sup ported in a future release. Some of the host-side utilities are also not supported in the restricted security world modes.

Loading a previously created Security World onto v12.50 firmware will work as usual, but many of the new features (like Audit Logging) will not be available.

4.3. User Interface support

Security World v12.50 continues to ship with a number of different user interfaces for using

and managing the product. However, only the command line tool has been updated to support creating new Security Worlds. As such, other UIs (nShield Connect Front Panel, KeySafe and the CAPI wizards) should not be used for creating a new Security World with this release.

4.4. Versioning

Security World v12.40 introduced a new versioning scheme for components in the nShield Security World release. Security World v12.50 expands this versioning to all updated components; as such all firmware images, Connect images and host-side software will report 12.50.2 or 12.50.4 as their version number.

Note: Additional information is reported after the v12.50 version number, which is used to identify specific build information. This information should be referenced when seeking support from nshield.support@entrust.com.

5. Upgrading from previous releases

5.1. Installing v12.50 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 Unix platforms, except Solaris 11, if you have applications built against previous ver sions of nflibs, in order to maintain backwards compatibility, you must create the file `/etc/nfast.conf` with the entry `NFAST_CREATEDEVNFAST=1`. This will create the symlink `/dev/nfast` (which points to `/opt/nfast/sockets`) during the start-up sequence.

For details of how to install the v12.50 Security World software, refer to the Chapter: *Installing the software*, in the appropriate *Installation Guide*.

5.2. Upgrading nShield Solo XC Firmware

If the Solo XC HSM is installed with the earlier 3.3.10 firmware it cannot be upgraded directly to the latest firmware and needs to be first upgraded to an intermediate firmware. Please contact support and request the firmware upgrade patch from 3.3.10 to 3.3.20.

If the Solo XC HSM is installed with firmware earlier than 12.50.2, 3.4.2 or 3.3.41 it cannot be upgraded directly to the latest firmware and needs to be first upgraded to an intermediate firmware. Please contact support and request the firmware upgrade patch

5.3. Latest v12.50 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 latest firmware is provided on the install media and should be installed on an nShield HSM in accordance with **Table 2** and **Table 3**.

All of the latest 12.50.2 versions of firmware will not be submitted for FIPS certification. A new version of firmware superseding 12.50.2 will be submitted for FIPS certification in the near future. For the latest informa

tion on the FIPS status of this firmware please contact nshield.support@entrust.com

For security reasons, the VSN of the nShield Firmware and nShield Connect image file was increased (see **Table 2** and **Table 3** below). Increasing the VSN ensures that once the nShield Firmware or the nShield Connect image file from v12.50 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 nshield.support@entrust.com if you require further information

Table 2 Latest firmware image files provided on v12.50 install media

HSM	Directory location on the install media	VSN
nShield Solo, nShield Solo+	Monitor: `/firmware/2-60-1/ldb_ncx3p-26.nff` Firmware: `/firmware/12-50-2/ncx3p-29.nff`	29
nShield Edge	Monitor: `/firmware/2-50-16/ldb_ncx1z-24.nff` Firmware: `/firmware/12-50-2/ncx1z-29.nff`	29
nShield Solo XC	`firmware/12-50-2/ncx5e-37.nff`	37

Table 3 Latest nShield Connect image files provided on v12.50 install media

HSM	Directory location on the install media	Firmware version	VSN
nShield Connect, nShield Connect+	`nethsm-firmware/12.50.4cam4/nCx3N.nff`	12.50.2 (VSN = 29)	31
nShield Connect XC	`nethsm-firmware/12.50.4cam4/nCx3N.nff`	12.50.2 (VSN = 37)	31

5.4. FIPS approved firmware and nShield Connect image

In the event that you wish to use Security World v12.50 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 4 and Table 5 below.

All of the firmware versions listed below are FIPS certified versions

Table 4 FIPS approved/pending firmware and image files provided on v12.50 install media

HSM	Directory location on the install media	VSN
nShield Solo, nShield Solo+	Monitor: `/firmware/2-60-1/ldb_ncx3p-26.nff` Firmware: `/firmware/2.61.2/ncx3p-26.nff`	29
nShield Edge	Monitor: `/firmware/2-50-16/ldb_ncx1z-24.nff` Firmware: `/firmware/2.61.1/ncx1z-26.nff`	29
nShield Solo XC	`firmware/3.4.2/ncx5e-37.nff`	37

Table 5 FIPS Connect image files provided on v12.50 install media

HSM	Directory location on the install media	Firmware version	VSN
nShield Connect, nShield Connect+	`nethsm-firmware/12.50.4cam4-fips/nCx3N.nff`	2.61.2 (VSN = 29)	31
nShield Connect XC	`nethsm-firmware/12.50.4cam4-fips/nCx3N.nff`	3.4.2 (VSN = 37)	31

6. Compatibility

6.1. Supported hardware

This release is targeted at deployments of any combination of the following 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

6.2. Supported operating systems

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

Table 6 Supported operating systems

Operating System	Solo+	Solo XC	Connect+ Connect XC	Edge
Microsoft Windows Server 2016 Core 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	Y	N	Y	Y
Red Hat Enterprise Linux AS/ES 6 x64	Y	Y	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

Operating System	Solo+	Solo XC	Connect+ Connect XC	Edge
Oracle Enterprise Linux 7.1 x64	Y	Y	Y	Y

Security World v12.60 Linux support is restricted to x86/x64 architectures. Additional mainstream x86/x64 based Linux distributions other than those listed above may be compatible, however Entrust cannot guarantee this compatibility.

6.3. Supported virtual environments

Table 7 Supported operating systems

Operating System	Solo+	Solo XC	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

6.4. Supported compilers for Microsoft Windows C developers

Security World v12.50 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 Stu dio (i.e. 2010 and earlier).

Microsoft Windows developers using CipherTools or CodeSafe should upgrade to Visual Studio 2013.This applies primarily to static libraries.

6.5. 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 nshield.support@entrust.com.

6.6. Impath protocol compatibility

The Impath protocol is used to secure nShield Connect, RFS (Remote File System) and Remote Operator communication. v12.50 has extended the protocol to include a new CipherSuite DHPrime3072Ex which will be used when both peers are using v12.50 software/firmware.

Backwards compatibility with previous versions is supported except for the datalimit and timelimit configuration options which are now obsolete. The following advice for maximum compatibility between versions applies to both Security World v12.50 and pre-v12.50 configuration files:

- The `datalimit` and `timelimit` fields should both be set to `0` in the hardserver configuration file (`/opt/nfast/kmdata/config/config` or `%NFAST_KMDATA%\config\config`) and in the `hs_clients` section of nShield Connect configuration files.
- Impath resilience should be enabled in Connect configurations (this is the case by default, so unless it has been explicitly disabled no additional configuration is required). Impath resilience is configured with the `enable_impath_resilience` field in the `nethsm_settings` section of the nShield Connect configuration file.

6.7. CodeSafe

6.7.1. Supported development platforms

In Security World v12.50, CodeSafe development is only supported on:

- Microsoft Windows
- Red Hat Enterprise Linux
- SUSE Enterprise Linux

CodeSafe applications can still be deployed on any OS supported by Security World.

6.7.2. 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 Makefile-examples file within the glibsee examples directory in the CodeSafe SDK for guidance on the new build parameters; and see the *CodeSafe Developer Guide* and the API documentation for information on any API changes.

6.7.3. 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.

7. Defect Fixes

7.1. Defect fixes in client-side software

Table 8 Client-side defects fixed in v12.50.2 & v12.50.4

Reference	Description
NSE-15165	When unplugging a nShield Edge from its host a script error may be logged in the edgeHandler.log file. This has now been resolved.
NSE-15108	Fixed an issue on Windows platforms that caused the raserv process with the "-c" or "-L" options to crash.
NSE-14427	generatekey failed to generate PKCS#11 keys if an ACS card was in the slot. This is no longer the case
NSE-14012	Fixed an issue that could cause the hardserver to abort when running CodeSafe applications.
NSE-14190	A successful call to C_GetOperationState failed to set the length pulOperationStateLen, leaving it as the value passed in. This has been corrected.
NSE-13995	Fixed an issue in the GnuPG patch for integrating with nShield hwcrhk which could cause an assertion failure.
NSE-13590	When a badly-formatted ECDSA signature was presented to the nShield JCE provider, an Exception with an incorrect error message was thrown. The 'expected' and 'got' values were reversed. This has now been corrected.
NSE-13332	A number of race conditions were identified in multi-threaded use of nCipherKM. The relevant code is now protected by mutexes.
NSE-13477	Fixed an issue where the Remote Administration Client GUI or raccmd tool could fail due to incorrect processing of network messages.
NSE-13102	Fixed an issue in the nFast Server service that caused Windows machines to wake from sleep mode.
NSE-13370	Fixed an issue in the nShield JCE provider that prevented MGF1 algorithms being usable with Java's {{keytool}} due to failure to declare the OID for those algorithms.
NSE-12799	Previously, the online help for Cmd_SetNSOPerms did not include NSOPerms_ops_OriginateKey in the list of public permissions that should not be set to fully comply with FIPS 140-2 level 3. This has now been corrected.
NSE-12747	Malformed commands or commands with invalid data could remain on the list of commands awaiting reply indefinitely, impacting performance of programs using nfjava or the nCipherKM JCE provider. Such commands are now removed from the list when detected. The list has also been reimplemented to reduce the impact of large numbers of waiting commands.

Reference	Description
NSE-12509	JCE CSP certificates have been upgraded to RSA 3072-bit with SHA-256. Note that this requires the following patch levels for Java: 9/8u111/7u121/6u131 (October 2016) and later.
NSE-12556	Our PKCS#11 library advertised a limit of 4096 bits for RSA keys despite being capable of handling longer keys. The advertised limit has been raised to 8192 bits.
NSE-12493	Previously, by default the nFast Server service on Windows accepted privileged local connections from any user, unless explicitly restricted with the nt_privpipe_users field in the config file. Now the default has been changed so that only processes with local administrative privilege are allowed to issue privileged connections to nFast Server on Windows by default. The nt_privpipe_users field continues to be available in config to enable a user-specified user or group to be permitted to make privileged connections. See also notes below for outstanding issue NSE-11885.
NSE-11821	Losing communication with a single HSM could cause C_GetSlotList to fail. C_GetSlotList has been made more robust.
NSE-11669	"The incorrect product name was reported for SoloXC and ConnectXC HSMs by enquiry. enquiry now reports: product name nC3025E/nC4035E/nC4335N"
NSE-11569	Strict FIPS mode on SoloXC does not permit the generation of 1024-bit RSA keys. ckcheckinst has been updated to use 2048 bit RSA and DSA keys.
NSE-11535	Fixed an issue in the nShield CNG Key Storage Provider where the NCryptEnumAlgorithms function did not list any algorithms unless an algorithm class was specified.
NSE-10681	NShield JCE CSP signatures now include a timestamp.
NSE-10632	Server permission mismatches were always reported, even when a matching permission was found. Now they are only reported when permission is not granted.
NSE-10586	Fixed an issue that could cause the hardserver service to get stuck in an infinite loop on Windows.
NSE-10584	Fixed an issue that could cause the hardserver to allocate large amounts of memory or abort.
NSE-10495	Fixed an issue where SoloXC devices would not be detected in machines with fast boot-up.
NSE-10335	The implementation of select() in BSDlib library for SEE mishandled errors on non-blocking streams, always returning EWOULDBLOCK in that case. This has been corrected.
NSE-10184	Java 8 made changes to the Sun PKCS11 provider, so that the key generation would fail in our PKCS#11 library, even with JCE Compatibility mode enabled. JCE compatibility mode has been changed to meet the new requirements.
NSE-9744	The generatekey utility now defaults to SHA-256 rather than SHA-1 for certification requests.
NSE-9745	The CodeSafe SEE machine signing tool incorrectly used SHA-1 to identify SEE machines being signed when signing with a stronger hash. It has been fixed to consistently use the same hash for signing and SEE machine identification.

Reference	Description
NSE-9674	Fixed an issue that prevented enquiry from reporting connection information for failed nShield Connects.
NSE-12118	Fixed an issue that prevented miniHSM-based nTokens from being recognized automatically on Windows.
NSE-11943	Nethsmadmin now returns a non-zero exit status if an image upgrade operation fails.
NSE-11909	"The deprecated CodeSafe SSL library has been removed. OpenSSL is available to CodeSafe applications using the supplied nShield patch for CodeSafe and is the recommended replacement for CodeSafe SSL."
NSE-11460	Fixed an issue in the CodeSafe developer tools that caused SEE machines to fail on SoloXC and ConnectXC.
NSE-11242	The nCipher MIB has been updated to allow 'softcard' as a valid option for key protection.
NSE-11053	Malformed FTSessionOpen commands were mishandled, potentially causing the hardserver to abort. This mishandling has been corrected.
NSE-11018	Fixed an issue that could cause the hardserver to abort in response to some port scanning tools.
NSE-10890	Corrected symlink configuration for nTokens on Linux to prevent an error being logged.
NSE-8202	Creating a DLf3072s256mRijndael ciphersuite Security World with remote administration sometimes failed with OperationTimeout. The default timeout for card_remove_detect_-time_limit has now been increased to address this.
NSE-8508	The OpenSSL patch supplied with the CodeSafe developer kit has been updated to support version 1.0.2o.
NSE-9393	The OpenSSL binaries bundled with nShield have been updated to 1.0.2o.
NSE-6745	Previously, the CNG Key Storage Provider logged failure to find a key with a given name as an error-level message in logs. It is now possible to configure whether such events are considered errors. See the *User Guide* for more information.
NSE-5938	ckcheckinst attempted to use RSA encryption with PKCS#1 V1.5 padding. This will fail in Security Worlds created with the --disablepkcs1pad option. ckcheckinst has been updated to use OAEP padding instead.
NSE-3621	The Remote Administration Client now attempts to establish an exclusive connection to the nShield Remote Administration Card. If an exclusive connection cannot be established, a shared connection to the card is made and a warning is displayed to the user regarding potential interference with Remote Administration operations from other processes.
NSE-12830	Fixed an issue that could cause the hardserver service to leak small amounts of memory.
NSE-6804	It is now enforced that the file {{/etc/nfast.conf}} is only writable by root if it exists.
NSE-2485	The Impath kx group DHPrime1024 is no longer supported. All Impath communication will now use DHPrime3072 or DHPrime3072Ex.

Reference	Description
NSE-15287	Improved the CodeSafe Developer examples.
NSE-1613	Improved the workflow in the CNG wizard workflow as part of the Softcards in CNG feature.
NSE-6010	Corrected an issue with perfcheck reporting results for Mid/High speed Solo XCs.
NSE-11686	The client application can loop infinitely because it fails to clean its command queue when the connection is broken. The fix removes these outstanding commands and marks them as failed.
NSE-15234	Previously nfkmverify incorrectly assumed that a key with a timeout cannot be protected with a non-persistent token or softcard. This has now been corrected.
NSE-4568	The hardserver on Windows was previously binding to all interfaces instead of just loopback for ports 9000/9001 used for local TCP client connections in some cases. TCP connections from external addresses were, however, rejected by the hardserver internally in spite of this. Now the hardserver binds to local loopback only for local TCP client connections.
NSE-4160	If CNG providers were manually uninstalled and then installed using the cnginstall utility whilst the provider DLLs were in use by a process, then the provider DLLs were installed incorrectly on next reboot. This has now been fixed, and the provider DLLs are now copied correctly on reboot. Installation and uninstallation with the cnginstall utility when the provider DLLs were not in use took immediate effect and was not affected by this issue.
NSE-3827	Previously, executables with non-ASCII characters in their path or name failed to connect to the hardserver with the error Status_Malformed. Now, non-ASCII characters in hardserver client paths and executable names are tolerated, but statistics information (e.g. as reported by stattree) will still show only ASCII characters for the process name in hardserver client connections.
NSE-1934	Fixed an issue in the nShield CAPI CSPs that could cause CryptDestroyHash to fail with error 0x57 "The parameter is incorrect".
NSE-11289	Solo XC now correctly returns the stattree MemAllocUser parameter when a SEE app is running (previously would always return 0)
NSE-10230	The Cmd_NVMemAlloc command only used the supplied file name up to the first zero byte, not respecting the length parameter. This has been corrected.
NSE-14148	When changing the MOI settings on a nShield Edge the hardserver sometimes generated an assert and exited. This has now been handled as an error.
NSE-14882	With a CodeSafe application running, HSMs were reporting a very high idle command count (shown via stattree). This has been corrected.
NSE-15528	When using HSP Pool mode, multiple "Notice: Calling transform_reply" messages could appear in the hardserver log. This has been corrected.
NSE-9064	Windows Authenticode timestamps use the SHA-256 digest algorithm in place of SHA-1.
NSE-12626	The deprecated function SEElib_StopTransactListener is no longer supported nShield HSMs.

7.2. Defect fixes in nShield Connect & Connect XC image file

This section contains details of defect fixes specific to the Connect HSM, however if the Connect is using the latest HSM firmware then the defect fixes in section 7.3 below also apply.

Table 9 Connect & Connect XC defects fixed in v12.50.4

Reference	Description
NSE-15289	Fixed an issue that prevented the module's monitor firmware from being updated when expected in nShield Connects.
NSE-10779	NShield Connect firmware upgrades were allowed to start which eventually failed due to VSN downgrade protections on internal components of the Connect. This aborted upgrade left the nShield Connect in an inconsistent but usable state. There is now a "pre-flight-check" to avoid starting nShield Connect firmware upgrades that cannot complete.
NSE-8920	Fixed an issue that prevented remote loading of SEE machines to an nShield Connect XC.
NSE-3684	Changed the way system time and date are set from the nShield Connect front panel so that a reboot is no longer required, avoiding time discrepancies that have been seen occasionally.
NSE-12006	Fixed an issue where an nShield Connect may fail to reboot after 50 upgrades.
NSE-16075	Fixed an issue where enabling audit logging, either explicitly or by creating a Common Criteria CMTS mode Security World, on an nShield Connect HSM could lead to the HSM becoming unresponsive

7.3. Defect fixes in Solo & Solo XC firmware

Table 10 Solo & Solo XC defects fixed in v12.50.2

Reference	Description
NSE-11839	The generation of RSA keys has been updated to ensure strict compliance to FIPS 186-4. Prior to this it was theoretically possible to generate a non-compliant key although the probability was so low that it is unlikely that such a key has ever been generated.
NSE-10522	DSA signature generation now performs the check and regeneration of the signature if r or s are equal to zero for compliance with FIPS186-4.
NSE-9964	KLF is no longer allowed in new Security Worlds created in 12.50 and has been replaced by KLF2

Reference	Description
NSE-9848	Diffie-Hellman (DH) keys produced prior to 12.50 were not strictly compliant to SP800-56Arev2. In 12.50 they have been replaced by a new key type, DHEX, that is compliant to SP800-56Arev2.
NSE-9598	A pairwise consistency check has been implemented in the OP_CRYPT operation for generated keys to ensure that the plaintext and ciphertext are different.
NSE-12031	Initiating loading a token from shares (Cmd_LoadLogicalToken) now sets the insertion time of the token to the current time.
NSE-11158	When using many different large RSA or DSA keys on Solo+ under heavy load the HSM may eventually fail. This issue was found with 8kbit keys but may also cause failures with other large key sizes.
NSE-10576	Fixed an issue with generating key pairs in CodeSafe in cases where the command takes more than 100 seconds to complete.
NSE-11409	Limited the memory statistics gathering to once every 30 minutes
NSE-1457	For nShield Solo and Solo+ added a memory-protection scheme to mitigate vector-rewrite attacks.
NSE-1339	Operations using the RIPEMD160 algorithm are now restricted from use when operating in a Security World created to be compliant to FIPS 140-2 level 3.
NSE-13268	Solo XC now records and reports the Max and Min temperature of the HSM (StatID_MaxTempC and StatID_MinTempC in stattree). This matches the behaviour of the Solo+ HSM.
NSE-13678	The Solo XC will no longer process any messages following a tamper event. This matches the behaviour of the Solo+ HSM.
NSE-13612	RSA Key generation performance has been improved on the Solo XC Base.
NSE-9761	KML signatures could use SHA-1 with 3072-bit keys. KML signatures can no longer use SHA-1 with 3072-bit keys
NSE-10245	In environments where an OCS card is left in a smartcard reader to authorise an ongoing operation, the continuous presence of the card may be mistakenly interrupted resulting in the removal of authorisation. This does not affect remote administration slots, or Remote Administration Ready smartcards (whether they are in remote administration slots or not). This does not affect persistent OCS. This defect was introduced in v12 firmware.

8. Known Issues

Table 11 Known issues in v12.50.4

Reference	Description
NSE-14406	In the Connect config file the remote_sys_log config entry implies multiple entries can be defined but only one remote syslog server can be configured.
NSE-14978	If Cmd_ChannelOpen is called without a key id an audit log message will be generated. This can occur if, for example, if Cmd_Hash is being used to hash a large amount of data. The nShield code translates this to opening a channel in Sign mode without a key. This would normally not be logged unless the key had the logkeyusage permission group flag. However, without a key the necessary checks cannot be performed and the Cmd_ChannelOpen is logged. This can be identified as a log entry without a key hash.
NSE-14519	The enquiry utility in v12.0 client-side incorrectly reports v12.50 Connect modules as Failed. This is a reporting error in this utility only and does not affect other applications. To confirm the module is in fact usable it is possible to send a NoOp command with: nopclearfail -n -m 1
NSE-15750	NTP reports "Error: ntpd timed out" in syslog 15 minutes after successful start-up - this does not indicate NTP has failed and can be ignored.
NSE-15826	The example audit-log-verifier.py program provided in the <NFAST_HOME>/python/examples folder and documented in the *Audit Logging* appendix of the *user guide* currently requires a Security World on the HSM being used to perform the verification whereas the *user guide* states that this is not required. Either ensure a Security World is present on the HSM being used for audit log verification or perform the following change to the example verifier program. Find the statement where the connection is made "self.conn = connection(needworldinfo=True)" and change the "needworldinfo" parameter to "False". This will be addressed in a future release.
NSE-14362	Type 0 smart cards cannot be used in a v12.50 FIPS level 3 enforced Security World. Contact Support if you need information on moving from type 0 smart cards to supported smart cards.
NSE-15284	With this release of the CodeSafe Developer Kit the build flags required for nShield Solo XC and nShield Connect XC have changed. It is essential that NF_CROSSCC is removed from all XC SEE Machine build configurations. See the examples in the developer kit for further details.
NSE-15748	Running cnglist.exe --list-keys --verbose causes the nShield CNG providers to crash.
NSE-15762	Some instability has been seen in the CNG nShield Service Agent when HSMs report failure after being cleared.
NSE-15822	NTP stops working after upgrading from v12.50.1 Preview release to v12.50.2 or later; the entry "Couldn't open </config/ntp/nto.server>" appears in the nShield Connect syslog. This will be addressed in a future release.

Reference	Description
NSE-15834	After disabling key recovery in a Security World (using killrecov), nfkmverify no longer verifies the Security World, reporting "ACL of NSO not of expected form". The Security World is still usable and key recovery has been disabled.
NSE-19300	Changes were made in 12.50 that mean the nShield Connect no longer prompts for a reboot following a change in time. This can lead to issues with logs no longer being pushed to the RFS. It is therefore recommended that when manually changing the time on the nShield Connect (especially into the past) that the nShield Connect is rebooted.
NSE-22187	CodeSafe applications running on a Solo XC or a Connect XC with high CPU usage can be terminated by the HSM's supervisory functions.
NSE-11380	Firmware version v12.50 for the nShield Solo XC HSM shows a drop in ECDSA digital signature performance compared to the FIPS 140-2 certified firmware version 3.4.2. Previously ECDSA operations used random numbers generated by the cryptographic accelerator. However as of v12.50 firmware, ECDSA operations use an Entrust-developed DRBG that has been qualified against NIST and German AIS-31 standards. Unfortunately this change results in reduced ECDSA performance.

9. Known issues from earlier Security World releases

Table 12 Known issues in previous Security World releases

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.
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.
NGSOL-2155 /NSE-4583	The slotinfo command returns the wrong card type for Unformatted Remote Administrator ready smart cards
NGSOL-2377	RSA Key Generation Fails when executed simultaneously on multiple VMs
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-2744 /NSE-9242	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 reapplied 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 conditions, 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 hard rebooted. It is not sufficient to just reboot the VM.

Reference	Description
NSE-7618	When a 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.
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.
NSE-11885	Hardserver ignores settings for nt_pipe_users/nt_privpipe_users if Java ports (local-loopback TCP) are open. This issue is not present when the hardserver is running in scaling mode.
NSE-11911	Solo and Solo+ behave differently to the SoloXC when restarting the hardserver in pre-maintenance 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.
NSE-7575	The user won't see the max exported modules being updated when running enquiry after remotely enabling the client licenses 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-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-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 issue does not affect 64-bit Linux systems.

Reference	Description
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.
NSE-2671	Codesafe SEELib "nvram" example SEE machine crashes on startup.
NSE-2899	CNG Wizard says "There was an error reading the card" when it means "card not in Authorized Card List".
MEI-4304 / NSE-3320	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 / NSE-3321	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 / NSE-3326	Applications that call NFKM_checkconsistency display "nfkmcheck: warning: World kmdata entry E0x199=E409 unexpected"
MEI-4386 / NSE-3328	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-3246	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.

Reference	Description
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.
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.
NSE-3738	Using Remote Operator to import a slot to an HSM running pre-v12.00 firmware from an HSM running v12.00 firmware or later results in getslotinfo and other utilities returning "Malformed". To avoid this issue do not use a mix of pre and post v12.00 HSM firmware with Remote Operator.
NSE-3743	Nfwarrant can fail silently, claiming it has generated a Certificate Signing Request (CSR) file when it has not. A particular instance of this is attempting to generate a CSR for a module that is part of a v12.50 Security World and in this case the module should be removed from the Security World first.
NSE-11828	Using the new-world utility without specifying a module results in it reporting incorrectly that it has generated a Security World on module #0. This can be avoided by specifying the module to use.
NSE-12095	CodeSafe applications on XC HSMs do not terminate when a thread calls ExitThread(456) / pthread_exit(). A workaround is to use the exit() system call.
NSE-13607	Attaching an nShield Edge and nShield Connects to the same Client computer or VM may result in a Connect being hidden from the enquiry utility. We do not recommend using the nShield Edge alongside other nShield HSMs on the same computer or VM.
NSE-14152	The bulkerase utility does not remove card files of Operator Card Sets that are more than 1/1, it only erases the single presented Operator card.

9.1. Known issues in older Remote Admin Client release

Table 13 Know issues in previous Remote Admin Client releases

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, e.g. 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.
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.
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.

10. Appendix A: Security Information

This appendix contains relevant security information applicable to this release and should be consulted prior to updating to v12.50.

10.1. Date and Time

The following sections provide procedural guidance about securely using date and time functions. Please see the *User Guides* for information on how to operate these functions.

10.1.1. Set the nShield Solo and Connect RTC

Set the Real-Time Clock (RTC) using an accurate trusted local time source as part of the commissioning process. This should be set as early in the commissioning process as possible. The correct time should be set to support hardserver and audit logging.

Note that the backup battery for the RTC on the nShield Solo and Solo+ will only last for two weeks when the module is not powered. The RTC must be reset on power up if the bat tery has drained.

10.1.2. Set the nShield Connect Date and Time

Set the nShield Connect date and time using an accurate trusted local time source as part of the commissioning process. This should be set as early in the commissioning process as possible. The correct time should be set to support system, hardserver and tamper logging. The nShield Connect supports a Network Time Protocol (NTP) client which if activated will synchronise the nShield Connect time to NTP. It is recommended that multiple NTP sources are requested to mitigate an attack on a single NTP source or failure of that source.

NTP suffers from a number of security vulnerabilities, see https://www.cvedetails.com/vulnerability-list/vendor_id-2153/NTP.html. The activation of NTP within the nShield Connect can increase the threats the nShield Connect is exposed to. Due to the nature of NTP design not all threats can be mitigated. NTP should only be used if your risk analysis identifies suitable controls to mitigate the impact of its operation. This could include

- Using only NTP servers that are under the control of the customer, i.e. within the customer's enterprise
- Using multiple NTP sources to mitigate an attack on a single NTP

> source or failure of that source.
>
> NTP can provide an accurate time source through consensus with multi ple input servers. It can also identify which available time servers are inaccurate

To further mitigate attacks on NTP the synchronised time should be compared against the Solo RTC time (including within the Connect) at regular intervals to ensure that a similar time, within a margin of error, is reported. Significant discrepancies should be investigated.

To identify NTP server failures or attacks, NTP servers should be monitored for availability on the network and an alert generated if the NTP server is unavailable.

10.2. Logging and Debugging

The following sections provide procedural guidance about securely using logging and debugging functions. Please see the *User Guides* for information on how to operate these functions.

10.2.1. Set Up Logging

Once the time has been set, your logging requirements should be identified and implemented. Various types of logs are available on nShield platforms:

Table 14 Logs on nShield Platforms - purpose and configuration

Log Type	Purpose	Configuration	NShield nToken	NShield Edge	NShield Solo+ and Solo XC	nShield Connect+ and Connect XC
Audit Logging	Operational and key usage activity	Can only be enabled at Security World initialisation	N	Y	Y	Y
Hardserver Log	Errors and troubleshooting	Controlled through environment variables. Default is to log nothing. Level of logging can be set.	Y	Y	Y	Y
Security World Log used by API libraries and base services	Errors and troubleshooting	Controlled through environment variables. Default is to log nothing, unless this is overridden by any individual library. If any of the four logging variables are set, all unset variables are given default values. Level of logging can be set.	Y	Y	Y	Y
System Log	System events on nShield Connect	Always enabled	N	N	N	Y
Tamper Log	Tamper events on nShield Connect	Always enabled	N	N	N	Y
Netsnmp Daemon Log	Netsnmp Daemon activity	Starts with the SNMP service. The SNMP Agent contains a Logfile switch to record warnings and message.	N	N	Y	Y

10.2.2. Audit Log

Only the Audit Log originates in the nShield Solo HSM (including the nShield Solo HSM installed in every nShield Connect). It uses a cryptographic mechanism to assure the integrity of the audit log distributed to third party SIEM Collectors.

- The SIEM Collectors should be located in a protected environment that limits physical access to the processing platform(s) on which the collector and validation applications are running to authorised Users.
- The availability of logs delivered to the SIEM Collectors should be maintained through a set of controls including:
  - Configuring multiple SIEM Collectors for each HSM
  - regular backups
  - physical and logical controls.
- A mechanism should be supplied to support the reliable delivery of logging messages to the SIEM Collectors.
- The network should be configured correctly to help prevent message corruption, congestion, forwarding loops, and incorrect delivery.
- The Audit Logging Verification process documented in the *User Guide* should be followed to verify Audit log entries. A process for supporting Audit Log Certification Block validation will be provided in a future release provided by Entrust to support the authenticated supply of a Trusted Root to the customer should be followed.
- Prior to shutting down the nShield Connect, a delay of at least 17 minutes should be made after the final log messages has been dispatched to the SIEM to ensure that the outstanding integrity verification message for those log messages is dispatched. The receipt of the verification message on the SIEM should be confirmed prior to shut down.
- In the event of a power failure or SOS on the nShield Connect, the integrity of any log messages that occurred after the last integrity verification message was dispatched cannot be verified. These log messages can potentially be altered or lost.

The Auditor should inspect the logs to:

- identify missing logs
- verify the integrity of logs up to the trusted root
- identify log entries that are a cause for concern

10.2.3. nShield Connect System and Hardserver Logs

The nShield Connect's System and Hardserver Logs can be stored within the nShield Con-

nect's tamper response boundary or pushed out to the RFS. If the logs are stored within the nShield Connect they will be protected by the tamper response boundary but will be lost if the nShield Connect is rebooted. Logging stops when the file system is full.

Alternatively, the logs can be pushed to a remote file system. However, no integrity mechanism is applied to the logs and therefore the customer should implement a trusted delivery and storage mechanism to protect the integrity of these logs if threats may arise in the network and storage environment that could compromise log integrity.

10.2.4. nShield nToken, nShield Edge, and nShield Solo Hardserver Logs

For nShield nToken, nShield Edge, and nShield Solo products the hardserver logs are stored in the associated host platform and do not have an integrity mechanism applied to the logs. Therefore, physical and logical controls should be applied to the host platform environment to protect the integrity of the logs.

10.2.5. Hardserver and System Log Environment Variables

For Hardserver and System logging, environment variables can be applied to control the amount of logging information. See the *nShield Connect* or *nShield Solo User guides* for more information. Your system management policy and security policy will determine the level of logging required.

10.2.6. nShield Connect Tamper Log

The nShield Connect's Tamper Log is located within the nShield Connect and protected by the nShield Connect's tamper mechanisms. It cannot be erased.

10.2.7. Time displayed in Logs

The Date and Time section above provides guidance on safely setting the time for the nShield Connect and RTC clocks. If NTP is enabled then the nShield Connect clock will synchronise to that. Both clock times will appear in the Audit Log and other logs described above. The nShield Connect (if not synchronised to NTP) and RTC are subject to drift and should be regularly set using an accurate trusted local time source.

With regard to the Audit Log we recommend only accepting that the nShield Connect and RTC time stamps represent the actual time if they match each other within a reasonable margin of error.

10.2.8. Debugging options

Debugging information is available for Hardware, Application, APIs, and Operating Systems. Unless required for development debugging for these sources should not be enabled (by default it's disabled).

Some debug information is provided in command line responses and therefore cannot be disabled.

CodeSafe debugging is disabled by default, but you can choose whether to enable it for all users or whether to make it available only through use of an ACS

Debugging can leak security information so should not be enabled in production environments.

10.3. Key Management

Key management is a critical component of a security product. A risk analysis will determine the strength of cryptographic algorithm and associated key sizes and lifetimes required to protect customer data.

10.3.1. Key Management Schema

Refer to the Security Worlds chapter in the *User guide* for a description of the Security World infrastructure available for managing the secure life-cycle of cryptographic keys. Refer to the Security World Access Control Architecture section for a description of the dif ferent keys available to protect application keys.

10.3.2. Security World Security Strengths

Security strength is represented by a number associated with the amount of work (that is, the number of guesses) that is required to break a cryptographic algorithm or system. The security strength is specified as a number of bits, typically from the set {80, 96, 112, 128, 192, 256}. For example, a security strength of 112 bits would require on average 2112-1 opera tions to break the security of the algorithm or system by brute force.

Security World modes are selected when creating a Security World. In v12.50 the available modes, associated cipher suites, automatic FIPS mechanism compliance and security strengths are:

Table 15 Modes, ciphersuites, FIPS mechanism conformance and security strengths available in v12.50

Modes	Ciphersuite	Automatic compliance of FIPS mechanisms with NIST SP800-131A Revision 1 algorithm/key sizes	Security Strength
FIPS 140-2 Level 3 (FIPS approved mode enforced)	DLf3072s256mAESc-SP800131Ar1	Y	128 bits
Unrestricted (default)	DLf3072s256mAESc-SP800131Ar1	N [1]	128 bits
Common Criteria CMTS [2]	DLf3072s256mAESc-SP800131Ar1	N	128 bits

[1] In this mode non-approved security functions (e.g. algorithms, primes) that are not compliant with NIST SP800-131A Revision 1 are available and if selected then the customer will be operating outside of a FIPS approved mode of operation (a mode of the cryptographic module that employs only Approved security functions).

[2] Common Criteria EN 419 221-5 Protection Profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services

Pre v12.50 Security Worlds can be loaded on to a v12.50 nShield Edge, nShield Solo on nShield Connect. The cipher suites, automatic FIPS mechanism compliance and security strengths for these worlds are:

Table 16 Pre-12.50 Security Worlds ciphersuites, FIPS mechanism conformance and security strengths that are available in v12.50

Modes	Ciphersuite	Automatic compliance of FIPS mechanisms with NIST SP800-131A Revision 1 algorithm/key sizes	Security Strength
Pre v12.50 Security Worlds	DLf3072s256mRijndael	N	128 bits [1]
	DLf1024s160mRijndael	N	80 bits
	DLf1024s160mDES3	N	80 bits

[1] Whilst the Cipher suite provides 128 bits of security strength some of the underlying, not selectable, cryptographic mechanisms pre v12.50 provide a reduced security strength. This is identified by the 'X' in the Compliance with FIPS mechanisms column.

Security strength is represented by a number associated with the amount of work (that is,

the number of guesses) that is required to break a cryptographic algorithm or system. The security strength is specified as a number of bits, typically from the set {80, 96, 112, 128, 192, 256}. For example, a security strength of 112 bits would require on average 2112-1 opera tions to break the security of the algorithm or system by brute force.

Security World modes are selected when creating a Security World. In v12.50 the available modes, associated cipher suites, automatic FIPS mechanism compliance and security strengths are: Table 15 and Table 16 identify the cipher suites, automatic compliance with NIST SP800-131A Revision 1 and security strengths. The National Institute for Standards and Technology (NIST) have published, over the years, good key management guidance. SP800-131A Revision 1 - 'Transitioning the Use of Cryptographic Algorithms and Key Lengths' is referenced in the table as it provides guidance on suitable cryptographic algo-rithms and key sizes for protecting sensitive data today. This document, published in November 2015, advises that the minimum security strength for algorithms or keys is now 112 bits. Whilst the immediate audience is U.S. government agencies, NIST standards pro-vide a global benchmark in security standards which many global product vendors adhere to, in order to provide their customers with appropriate levels of security assurance. There-fore, the industry standard minimum security strength is considered to be 112 bits today.

10.3.3. Application Keys, Algorithms, Key Sizes

Depending on the application library used, a range of cryptographic algorithms are available for selection. The algorithm used and key size selected (if applicable) should be sufficient to protect your data (or the data you control) from threats identified in the deployed environ-ment. In terms of security strengths, as described above in the Security World Security Strengths section, the security strengths applied need be no greater than the security strength of the Security World ciphersuite. As advised in the Security World Security Strengths section a minimum security strength of 112 bits is considered the industry stan-dard.

The Cryptographic Algorithms appendix in the *User Guide* identifies all algorithms and key sizes available (both NIST approved and unapproved). NIST SP 800-57 Part 1 Revision 4 has a section on Comparable Algorithm Strengths which provides guidance on identifying the security strength of different NIST approved algorithms and key sizes. BlueKrypt Crypto-graphic Key Length Recommendation is a useful reference for determining required key sizes for common cryptographic functions:

- Symmetric algorithms
- Asymmetric algorithms, based on the following branches of cryptography:
    - Factoring Modulus, such as RSA.

    - Discrete Logarithm Key/Group, such as DSA, Diffie-Hellman.
    - Elliptic Curve, such as ECDSA.
- Hashes

The General Key Management Guidance section of NIST SP 800-57 Part 1 Revision 4 provides guidance on the risk factors that should be considered when assessing cryptoperiods and the selection of algorithms and keysize.

The `nfkmverify` command-line utility can be used to identify algorithms and key sizes (in bits). See the Cryptographic algorithms appendix in the *User Guide* for more information.

10.3.4. Cryptoperiods

A cryptoperiod is the time span during which a specific cryptographic key is authorized for use. NIST SP 800-57 Part 1 Revision 4 has sections describing the rationale for cryptoperiods and the risk factors that should be considered when determining cryptoperiods. Setting a cryptoperiod limits, amongst other things, the amount of data exposure if a key is compromised. Customers are advised to perform a threat analysis, considering the sensitivity of their data and what controls they have in place to mitigate compromise, to determine appropriate cryptoperiods for keys protecting that data.

In terms of the Key Management Schema the following cryptoperiod rules must be applied:

- Application Keys must have a cryptoperiod assigned to them
- The Security World must have a cryptoperiod, as the Security World Keys (for example, Module Keys) are used to protect Application Keys. The cryptoperiod of the Security World must therefore be greater than or equal to the cryptoperiod of any Application Key.
- Whenever an Application Key reaches the end of its cryptoperiod it must be revoked. Whenever a Security World reaches the end of its cryptoperiod, a new Security World must be initialised and new Application Keys generated
- Cryptoperiods can be managed manually by deleting a key when it is no longer compliant with a customer's cryptoperiod policy. A key time out value can be applied to an Application Key to set its cryptoperiod (see for example the documentation for mkaclx in appendix C of the *User Guide*). In addition, the usage count can also be set for an Application Key. In a common criteria cmts Security World the maximum key timeout parameter can be used to control the maximum life of any Application Key, and the key usage parameter can be used to control the maximum number of times any Application Key can be used.