nShield Security World

nShield Security World v12.81 Release Notes

05 April 2024

Table of Contents

1. Release notes

1.1. Introduction

These release notes apply to the release of version 12.81 of Security World Software for the nShield family of Hardware Security Modules (HSMs). They contain information specific to this release such as new features, defect fixes, and known issues.

Security World Software and CodeSafe Developer Software are for users of nShield Solo (PCI Express variants), nShield Connect, and nShield Edge.

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

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

1.1.1. Purpose of Security World 12.81

Security World version 12.81 introduces enhancements as described in this document. It also corrects a number of defects that have been identified in earlier releases.

This release contains updates to the following products:

- Security World Software (including updated Connect images)

1.1.2. Versions of these Release Notes

Revision	Date	Description
1.1	2024-4-5	URL syntax fix for the HTML version. No content changes.
1.0	2022-11-31	Release notes for the first release of v12.81; v12.81.2

1.2. Product versions

1.2.1. Security World software versions

Version	Date	Description
v12.81.2	2022-03-28	First release of 12.81 Security World Software

1.2.2. Firmware and nShield Connect ISO versions

Version	Date	Description
v12.81.2	2022-03-28	First release of 12.81 Firmware and Connect ISO, including the release of firmware (12.80.5) and nShield Connect image (12.81.2) along with FIPS and CC approved firmware and Connect images.

1.2.3. nShield Firmware versions

Version	Date	Description
v12.80.2	2021-11-23	Release of 12.80 Firmware for Solo+ HSMs not updated since 12.80 release
v12.80.5	2022-02-28	Release of 12.80 Firmware for Solo XC HSMs not updated since 12.80 update release.

1.2.4. nShield Connect image versions

Version	Date	Description
v12.81.2	2022-03-28	First release of nShield Connect images for 12.81 containing the latest features and fixes.

1.3. Features of Security World v12.81

1.3.1. Remote Operator and Remote Administration

Security World v12.81 now allows both Remote Operator and Remote Adminstration to be configured concurrently for nShield HSMs. Previously they were mutually exclusive.

This release supports both usage in parallel where dynamic slots and Remote Operator slots can be configured on the same HSM and usage in series where a dynamic slot can be exported as a Remote Operator slot between HSMs.

Entrust recommends to configure complex Remote Operator and Remote Administration scenarios for the nShield Connect in the Connect configuration file. You can then pull the edited configuration file to the Connect using the front panel or push it to the Connect from the RFS with the `cfg-pushnethsm` utility.

For more information, see the Remote Operator and Remote Administration sections of the *User Guide* for your HSM.

1.3.2. CKM_RSA_AES_KEY_WRAP support in the nShield PKCS #11 API

Support for the `CKM_RSA_AES_KEY_WRAP` mechanism has been added to the nShield PKCS #11 API.

The mechanism is not supported for use with target keys when `CKA_WRAP_WITH_TRUSTED` is set. If `CKA_UNWRAP_TEMPLATE` is set on the RSA key, then `CKM_RSA_AES_KEY_WRAP` must be explicitly enabled for use in the key's `CKA_ALLOWED_MECHANISMS` attribute list and by setting `unwrap_rsa_aes_kwp` in `CKNFAST_OVERRIDE_SECURITY_ASSURANCES`.

Use of this mechanism requires 12.60.2 firmware or greater.

For more information, see the nShield PKCS #11 API sections of the *User Guide* for your HSM and the *Cryptographic API Integration Guide*.

1.3.3. AES-GCM support in the nShield PKCS #11 API

Support for the `CKM_AES_GCM` Wrapping mechanism has been added to the nShield PKCS #11 API.

For more information, see the nShield PKCS #11 API sections of the *User Guide* for your HSM and the *Cryptographic API Integration Guide*.

1.3.4. DH/ECDH key agreement in the nShield PKCS #11 API

This release introduces improvements to non-KDF DH and ECDH operations in the nShield PKCS #11 API. These improvements are not user visible and require both 12.80+ firmware and keys generated using 12.81+ releases of the Security World software. If this configuration is not available, the behavior will be as previous releases.

Support is provided for selecting either the most or least significant bits of the

derived key. The existing behavior of selecting the most significant bits is the default. If the environment variable `CKNFAST_DH_LSB` is set the least significant bits will be used.

For more information, see the nShield PKCS #11 API sections of the *User Guide* for your HSM and the *Cryptographic API Integration Guide*.

1.3.5. SHA-3 support in the nShield PKCS #11 API

Support for SHA-3 hashing functions has been added to the nShield PKCS #11 API. The following PKCS #11 hashing and ECDSA signature mechanisms are now supported.

- CKM_SHA3_224
- CKM_SHA3_256
- CKM_SHA3_384
- CKM_SHA3_512
- CKM_ECDSA_SHA3_224
- CKM_ECDSA_SHA3_256
- CKM_ECDSA_SHA3_384
- CKM_ECDSA_SHA3_512

For more information, see the nShield PKCS #11 API sections of the *User Guide* for your HSM and the *Cryptographic API Integration Guide*.

1.3.6. Additional SHA-2 ECDSA Signature Mechanisms in the nShield PKCS #11 API

The following SHA-2 ECDSA Signature Mechanisms have been added to the nShield PKCS #11 API.

- CKM_ECDSA_SHA224
- CKM_ECDSA_SHA256
- CKM_ECDSA_SHA384
- CKM_ECDSA_SHA512

For more information, see the nShield PKCS #11 API sections of the *User Guide* for your HSM and the *Cryptographic API Integration Guide*.

1.4. Firmware, nShield Connect images, and certifications

Security World 12.81 does not include the firmware and nShield Connect image files in the standard Security World or CodeSafe ISOs. Instead, an nShield firmware and nShield Connect image ISO is available which contains all firmware and nShield Connect images supported by this release. This ISO can be obtained through contacting https://nshieldsupport.entrust.com (asking for product code `SW2187C-FW`).

1.4.1. Firmware

There is no change to the installation of the firmware in 12.81.

To install the updated firmware run the installed `loadrom` utility pointing at the required firmware file on the ISO (or copy the firmware from the ISO to a local location).

1.4.1.1. nShield Solo+ firmware

Type	Version	Description	Directory	VSN
CC Approved	2.55.1	The latest CC approved firmware for 11.72. This should be used with Security World 11.72.02 on the client host	`/firmware/2-55-1/ncx3p-29.nff`	29
FIPS Approved	12.50.8	The latest FIPS approved firmware released as part of the v12.50 release.	`/firmware/12-50-8/ncx3p-29.nff`	29
Latest	12.80.2	Latest firmware with features and defect fixes from v12.80 release.	`/firmware/12-80-2/ncx3p-29.nff`	29

The firmware monitor to use with the above nShield Solo+ firmware: `/firmware/2-60-1/ldb_ncx3p-26.nff`.

1.4.1.2. nShield Solo XC firmware

Type	Version	Description	Directory	VSN
CC Approved	12.60.15	The 12.60 firmware currently certified to the CMTS Common Criteria certification	`firmware/12-60-15/ncx5e-37.nff`	37
FIPS Approved	12.50.11	The latest FIPS approved firmware released as part of the v12.50 release.	`firmware/12-50-11/ncx5e-37.nff`	37
Latest	12.80.5	Latest firmware with features from v12.80 release.	`firmware/12-80-5/ncx5e-37.nff`	37

1.4.1.3. nShield Edge Firmware

There is no updated 12.80 firmware for the nShield Edge. Support for the Edge is still maintained for previous firmware releases.

Type	Version	Description	Directory	VSN
FIPS Approved	12.50.8	The latest FIPS approved firmware released as part of the v12.50 release.	`/firmware/12-50-8/ncx1z-29.nff`	29

The firmware monitor to use with the above nShield Edge firmware: `/firmware/2-50-16/ldb_ncx1z-24.nff`.

1.4.2. nShield Connect images

The nShield firmware and nShield Connect Image ISO includes 12.81 nShield Connect images that contain the Solo+ and Solo XC firmware described in nShield Solo+ firmware and nShield Solo XC firmware. The following nShield Connect images are available as part of the 12.81 release which contain the FIPS approved HSM firmware.

1.4.2.1. Install an nShield Connect image

Previously nShield Connect images were provided on the Security World Software ISO (as part of the `nhfw` package) which allowed them to be installed into `/opt/nfast/nethsm-firmware` ready to be installed onto the Connect image.

Now that these images are not on the Security World ISO these need to be manually copied into the correct location.

As part of the Security World installation the `/opt/nfast/nethsm-firmware` directory is created, but is empty.

Once the nShield Connect image that needs to be installed is chosen, the subdirectory, that is `12-81-2-fips`, and the image should be copied from the nShield firmware and nShield Connect ISO into the `/opt/nfast/nethsm-firmware` directory and installed onto the nShield Connect as usual.

1.4.2.2. nShield Connect+ images

Type	Version	Description	Firmware included	Directory	VSN
CC Approved	12.45.1	nShield Connect image with CC approved 11.72 firmware	2.55.4	`nethsm-firmware/12-45-1/nCx3N.nff`	30
FIPS Approved	12.81.2	12.80 nShield Connect image with FIPS approved firmware	12.50.8	`nethsm-firmware/12-81-2-fips/nCx3N.nff`	31
Latest	12.81.2	12.80 nShield Connect image with latest 12.80 firmware	12.80.2	`nethsm-firmware/12-81-2/nCx3N.nff`	31

1.4.2.3. nShield Connect CLX images

Type	Version	Description	Firmware included	Directory	VSN
FIPS Approved	12.81.2	12.80 nShield Connect image with FIPS approved firmware	12.50.8	`nethsm-firmware/12-81-2-fips/nCx3N.nff`	31
Latest	12.81.2	12.81 nShield Connect image with latest 12.80 firmware	12.80.2	`nethsm-firmware/12-81-2/nCx3N.nff`	31

1.4.2.4. nShield Connect XC images

Type	Version	Description	Firmware included	Directory	VSN
CC Approved	12.80.4	12.80 nShield Connect image with CC approved XC firmware	12.60.15	`nethsm-firmware/12-80-4-cc/nCx3N.nff`	31
Transition Image	12.50.4	12.50 nShield Connect image with FIPS firmware to support transition between old and latest Connect images. See Upgrade an nShield Connect XC image for more information.	3.4.2	`nethsm-firmware/12-50-4-fips/nCx3N.nff`	31
FIPS Approved	12.81.2	12.81 nShield Connect image with FIPS approved firmware	12.50.11	`nethsm-firmware/12-81-2-fips/nCx3N.nff`	31
Latest	12.81.2	12.81 nShield Connect image with latest 12.80 firmware	12.80.5	`nethsm-firmware/12-81-2/nCx3N.nff`	31

1.5. Upgrade from previous releases

1.5.1. Install 12.81 Security World Software

Before installing this release, you must:

- Confirm that you have a current maintenance contract that licenses you to deploy upgrades on each nShield HSM and corresponding client operating system.
- Uninstall previous releases of Security World Software from the client machines.

For instructions, see the *Installation Guide* for your HSM.

1.5.2. Upgrade nShield Solo XC firmware

The following are important notes to observe when upgrading the Solo XC firmware to the latest version:

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 version. Please contact nshield.support@entrust.com and request the firmware upgrade patch from 3.3.10 to 3.3.20.

If the nShield Solo XC HSM is installed with firmware earlier than 12.50.7, 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 version. Any of the firmware versions listed above can be used as an intermediate version. Please contact nshield.support@entrust.com for any other version of firmware.

Whilst every effort is made to ensure nShield Solo XC firmware compatibility with all mainstream hardware and virtualized environments as well as operating systems there may be occasions where a particular configuration is not compatible (either through current version or after upgrading to a newer version of the firmware). Please contact nshield.support@entrust.com if you experience any issues following an upgrade or during integration activity.

1.5.3. Upgrade an nShield Connect XC image

If the nShield Connect XC HSM is installed with image earlier than 12.45, 12.46, 12.50.4, or 12.50.7 it cannot be upgraded directly to the latest nShield Connect image and needs to be first upgraded to an intermediate version. Any of the nShield Connect image versions listed above can be used as an intermediate version. Please contact nshield.support@entrust.com for any other version of nShield Connect image.

1.6. Compatibility

1.6.1. Supported hardware

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

- nShield Solo XC
- nShield Solo PCI Express (500+, and 6000+)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Connect CLX (Base, Mid, High)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield Edge
- nToken PCI Express "+" (NC2023E-000)

1.6.2. Supported operating systems

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

Operating System	Solo+	Solo XC	Connect	Edge
Microsoft Windows Server 2022 x64	Y	Y	Y	Y
Microsoft Windows Server 2019 x64	Y	Y	Y	Y
Microsoft Windows Server 2019 Core x64	Y	Y	Y	**N**
Microsoft Windows Server 2016 x64	Y	Y	Y	Y
Microsoft Windows 10 x64	Y	Y	Y	Y
Red Hat Enterprise Linux AS/ES 7 x64	Y	Y	Y	Y
Red Hat Enterprise Linux AS/ES 8 x64	Y	Y	Y	Y
SUSE Enterprise Linux 12 x64	Y	Y	Y	Y
SUSE Enterprise Linux 15 x64	**N**	**N**	Y	**N**
Oracle Enterprise Linux 7 x64	Y	Y	Y	Y
Oracle Enterprise Linux 8 x64	Y	Y	Y	Y

Security World v12.81 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.

1.6.3. Supported virtual environments

Operating System	Solo+	Solo XC	Connect	Edge
Microsoft Hyper-V Server 2016	N	Y	Y	N
Microsoft Hyper-V Server 2019	N	Y	Y	N
VMWare ESXi 6.7	N	Y	Y	N
Citrix XenServer 8.2	N	Y	Y	N

1.6.4. Supported compilers for Microsoft Windows C developers

Security World v12.81 C libraries for Windows were built using Visual Studio 2017 and have been compiled with the SDL flag. This makes them incompatible with older versions of Visual Studio. This applies primarily to static libraries.

Microsoft Windows developers should upgrade to Visual Studio 2017.

1.7. Option Pack support

Option Pack	Compatible Version
Database Security Option Pack (nDSOP)	To be confirmed
Cloud Integration Option Pack (CIOP)	v2.2.1
nShield Container Option Pack (nSCOP)	To be confirmed

Contact nshield.support@entrust.com for further information about the availability of any option pack.

1.8. Defect fixes

1.8.1. Defect fixes in client-side software

Reference	Description
NSE-42346	Fixed an issue where nShield Edge was not supported if there were also nShield PCIe devices installed

Reference	Description
NSE-40445	The IPv6 traceroute option on netui (1-1-1-8-2) is now consistent with the IPv6 ping menu in that, for IPv6 link-local addresses, the same interface selection sub menu (giving options for either Interface #1 or Interface #2) is displayed upon entering a fe80 prefixed address.
NSE-40020	Fixes issues with data handling in CKA_WRAP_TEMPLATE and CKA_UNWRAP_TEMPLATE to improve the handling of these templates and which could potentially lead to an application crash.
NSE-39263	PKCS#11 key generation failed in FIPS mode when CKA_UNWRAP_TEMPLATE was set.
NSE-37534	In previous releases there was a possible conflict between the version.properties file in nCipherKM.jar and a similarly named file in a third-party jar. The file has been renamed to ncversion.properties to avoid this.

1.8.2. Defect fixes in Connect+, Connect CLX, and Connect XC images

Reference	Description
NSE-1393	The nShield Connect can now import multiple remote slots via front panel

1.9. Known issues in Security World 12.81

See also Known issues from earlier Security World releases.

Reference	Description
NSE-44980	Imported remote slots are now allowed to be mapped to slot 0. The front panel dialogs have not yet been updated to indicate that both dynamic and remote slots are now allowed.
NSE-46075	As a result of changes to support Remote Operator and Remote Administration the cfg-remoteslots utility may abort if run when there is an existng entry with a slotid of 0. We recommend editing the config file directly to make changes to the configuration.

1.10. Known issues from earlier Security World releases

These issues are still present in 12.81.

Reference	Description
NSE-41442	Earlier versions of nShield Java had a bug related to the order of clean up for unused or out-of-scope key objects and would sometimes return Status_UnknownID for operations during long running nCipherKM JCE and nCore Java applications. The cause of this issue has now been fixed. Java applications that perform operations directly with KeyID values rather than key objects may see Status_ObjectInUse errors unless keys, tokens, merged keys and channels are destroyed in the correct "LIFO" order. Attempting to destroy a key or other object that is referenced by another object will result in Status_ObjectInUse errors. Eg, If an application loads a key and creates a channel with that key, nCore Java will now return Status_ObjectInUse if the application attempts to destroy the key before destroying the channel using that key.
NSE-42172	The Java examples shipped with Security World Software are designed for use with later versions of Java (specifically Java version 8 and above). The Java examples may not work in earlier versions. Security World Software v12.80 continues to support Java versions 7, 8 and 11
NSE-39545	There is a performance regression in using ECDSA over SECP160r1 in the 12.80 Solo+ firmware. THis does not impact the Solo XC 12.80 firmware. Larger curve performance is also not impacted. If SECP160r1 is used it is recommended to not upgrade the firmware to 12.80 on the Solo+.
NSE-42034	Cmd_Encrypt does not properly populate the returned M_IV structured for Mech_AESmGCM. If an IV was supplied to Cmd_Encrypt then this value can be used instead. If no IV was supplied to Cmd_Encrypt then, for Mech_AESmGCM, the default chosen has taglen=16 and aad=the empty byteblock.
NSE-39031	In Security World v12.10 a compliance mode was added to the nShield Connect to allow compliance with USGv6 or IPv6 Ready requirements. This mode changes the settings for the nShield Connect firewall so that it will pass-through packets which are discarded in the normal Default mode. This behavior is required for compliance testing but is not recommended for normal use since allowing packets with invalid fields or parameters through the firewall increases the attack surface. This mode is known not to function correctly in the v12.80 Connect Image and should not be enabled.

Reference	Description
NSE-41612	Downgrading an nShield Connect with the 12-80-3 Connect Image to an older version image with IPv6 networking configuration will require the nShield Connect to be factory reset following the upgrade. A new hardserver configuration file will also need to be created.
NSE-43519	12.80 clientside added support for IPv6 in the hardserver, however if IPv6 is disabled on the client machine the hardserver will fail to start. If IPv6 is disabled on the machine the following config item can be added to the Hardserver configuration file which will allow it to start: [server_remotecomms_ipv6] impath_port=0
NSE-36364	In rare cases upgrading from v12.50.x images to later v12.70 or v12.80 images can result in the Connect becoming stuck in maint2 mode and report 'hardserver error' on the front panel. This can be resolved by initiating a factory reset and a repeat upgrade to the intended Connect image to complete the process.
NSE-28462	During key migration, if an incorrect OCS passphrase is entered, the tool will output the message: + Error: Cannot migrate security world. + Failed to load softcard <card_name> : wrong passphrase The 'Error: Cannot migrate security world' message is erroneous and can be ignored. The tool will continue and reprompt for the correct passphrase. Once the correct passphrase is entered the key migration will continue and complete successfully.
NSE-28606	nCipher Security do not recommend migrating keys to non-recoverable Worlds since it would then be impossible to migrate the keys in future should the need arise. If keys are migrated into a non-recoverable Wold then it is not possibly to verify OCS and softcard protected keys directly with nfkmverify. The OCS or softcards must be preloaded prior to attempting to verify the keys.
NSE-24335	Note: This issue applies to 12.50.11 XC firmware only. As a result of work to improve the upgrade experience with Solo XC it is necessary to add the following lines to /etc/vmware/passthru.map for successful operation of Solo XC in an ESXi environment. # Solo XC 1957 082c link false
NSE-25477	If installing CAPI CSPs on Windows Server 2016 and 2019 do not select these as the default sChannel provider in the CSP wizards. If default sChannel is selected and the machine rebooted you will not be able to log in. It will be necessary to boot into safe mode and remove the CSPs as default sChannel providers.

Reference	Description
NSE-23982	While resetting password if user enters incorrect password, cli prompt prints lone "I". This is where login handler program would print "Incorrect password for cli" message. Only "I" gets through the wire in time due to slow baud rate of the connection. This error is trivial and is only seen at the first log in during password reset.
NSE-23412	Customers should download at minimum CMAKE 3.9 for their RHEL distribution to be able to build the shipped examples.
NSE-25401	When installing 12.60 on a Dell XPS 8930 PC, a "Files in Use" screen may be displayed where it prompts to close down and restart Dell, Intel and NVIDIA applications. This can be ignored.
NSE-25626	Cancelling a Windows installation of the nShield Software with the "nShield Trusted Verification Device" component selected may leave the CyberJack Base Components installed on the machine. The user must restart their machine and uninstall the CyberJack Base Components manually via Add/Remove programs to completely uninstall.
NSE-22337	Users installing on a Pre-Windows 10 machine should download the Windows KB2999226 update to ensure the nShield Software will install correctly.
NSE-26559	If there are symbolic links within the NFAST_KMDATA folder then the installation will pause. To rectify the issue remove any symbolic links that may exist within NFAST_KMDATA and re-run the installer.
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 12.0 client-side incorrectly reports 12.50/12.60 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-14362	Type 0 smart cards cannot be used in a FIPS level 3 enforced Security World (introduced in Security World v12.50). Contact Support if you need information on moving from type 0 smart cards to supported smart cards.

Reference	Description
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-15762	Some instability has been seen in the CNG nShield Service Agent when HSMs report failure after being cleared.
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.