Web Services Option Pack

WSOP v3.1.0 Release Notes

10 April 2024

Table of Contents

1. Introduction . . . 1
2. Features of nShield Web Service Option Pack 3.1.0 . . . 2
    2.1. New configuration options . . . 2
    2.2. Random number generation . . . 2
    2.3. Changes to existing WSOP functionality . . . 3
    2.4. MongoDB Key record format changes . . . 3
    2.5. New PKCS #11 functionality . . . 3
    2.6. Changes to existing PKCS 11 functionality . . . 4
3. Compatibility . . . 5
    3.1. Supported MongoDB versions . . . 5
    3.2. Supported hardware . . . 5
    3.3. Supported operating systems . . . 5
    3.4. Supported Security World versions . . . 5
    3.5. API version . . . 6
    3.6. API additions . . . 6
4. Defect Fixes . . . 7
    4.1. Known Issues . . . 8

1. Introduction

These release notes apply to version 3.1.0 of the nShield Web Services Option pack for Security World. They contain information specific to this release such as new features, defect fixes, and known issues.

2. Features of nShield Web Service Option Pack 3.1.0

2.1. New configuration options

The following configuration options have been added:

- New list keys endpoint configuration.

  The new `listkeys_max_limit` configuration option is relevant to the list keys endpoint only. When configured, it enforces a maximum limit of returned keys. Large queries can hurt the service.

- New cache options.

  In addition to the existing, general purpose `key_manager_inactivity` option, new settings have been introduced to allow greater control with memory management.

  - Independent capacity limits have been introduced for keys, groups, and protection domains
  - Independent 'Time-to-Live' periods can be set to control when items should expire and be unloaded from the HSM.

  > When the cache capacity limit is reached for keys and groups, the least recently used item will be evicted from the cache and unloaded from the HSM when additional keys or groups are loaded.

  > When the capacity limit is reached for Protection Domains, a `TooManyActiveDomains` error will be returned when attempting to activate additional Protection Domains. Active Protection Domains will never expire.

Please refer to the Configuration section of the User Documentation for more information on these new options.

2.2. Random number generation

A new endpoint for the generation of random numbers from the HSM is now available. The length of the random number is specified in bytes and the return value is encoded in base64RawURL format.

2.3. Changes to existing WSOP functionality

- Changes to Linux install paths.
  - Default corecrypto install path is now `/opt/nfast/webservices/corecrypto`.
  - Default corecrypto log file is now `/opt/nfast/log/corecrypto.log`.

2.4. MongoDB Key record format changes

This release introduces a change in the format of the MongoDB Key record, which is incompatible with previous versions of WSOP. A new `upgrade` option is now available in the Database Management Tool (DBMT) which will convert any existing databases from the previous v3.0.1 release of WSOP.

> When upgrading from version 3.0.1 to version 3.1.0, the DBMT `upgrade` option must be performed before the system is ready for use.

Please refer to the Database Management Tool section of the User Documentation for more information.

2.5. New PKCS #11 functionality

- Support for sign and verify functions.
  - `C_SignInit`
  - `C_Sign`
  - `C_VerifyInit`
  - `C_Verify`
- Generation of HMAC keys with `C_GenerateKey`
  - `CKK_SHA256_HMAC`
  - `CKK_SHA384_HMAC`
  - `CKK_SHA512_HMAC`.
- New HMAC and HMAC_GENERAL mechanisms for sign and verify.
  - `CKM_SHA256_HMAC`
  - `CKM_SHA256_HMAC_GENERAL`

  - `CKM_SHA384_HMAC`
  - `CKM_SHA384_HMAC_GENERAL`
  - `CKM_SHA512_HMAC`
  - `CKM_SHA512_HMAC_GENERAL`
- Updates to utilities
  - Added `ckcheckinst` utility.
  - Replaced `ckmechinfo-dynamic` with `ckmechinfo`.
- Added Windows support

  See Supported operating systems for more details.

2.6. Changes to existing PKCS 11 functionality

- Changes to Linux install path and file names.
  - Default install path is now `/opt/nfast/webservices/pkcs11`.
  - Default log file name is now `pkcs11webservices.log`.
  - Config file name is now `pkcs11webservices.cfg`.

3. Compatibility

3.1. Supported MongoDB versions

This release has been tested against MongoDB versions 4.4.10 and 5.0.13.

3.2. Supported hardware

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

- nShield Solo PCI Express (500+, and 6000+)
- nShield Solo XC (Base, Mid, High)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Connect XC (Base, Mid, High, Serial Console)

3.3. Supported operating systems

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

- Red Hat Enterprise Linux Server 7 x64
- Red Hat Enterprise Linux Server 8 x64
- Red Hat Enterprise Linux Server 9 x64
- SUSE Enterprise Linux 12 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 7.6 x64
- Oracle Enterprise Linux 8 x64

Additionally the PKCS #11 library has been tested for compatibility with the following operating systems:

- Windows Server 2019 x64
- Windows Server 2022 x64
- Windows 10 x64
- Windows 11 x64

3.4. Supported Security World versions

This release can be used with the following nShield Security World Software installations:

- Security World v12.80

> ℹ Security World v12.8x is required in order to migrate kmdata files using the Database Management Tool.

Firmware versions supported by the 12.60 release are also supported by WSOP. See the nShield 12.80 Security World Software release notes for further details.

3.5. API version

The nShield Web Service Option Pack REST API version has been increased to v1.3.0.

3.6. API additions

The following support has been added to the API:

Crt	Endpoint	Verb	Operation

1	`/random/v1/random-bytes`
	`/random/v1/random-bytes?length=n`
		`GET`	Generate random bytes from the HSM
			The generated random number is returned encoded in a base64RawURL format.
			This endpoint takes a single length input parameter, with a minimum value of 1 and a maximum value of 65535.
			If no length parameter is supplied, a default value of 1 will be used.

4. Defect Fixes

Reference	Description in v3.0	Fix in v3.1
NSE-48841	When C_FindObjects is called with CKA_VALUE_LEN in the search template, objects with values of CKA_VALUE_LEN not matching the search criteria could be returned.	Fixed an issue where calling C_FindObjects with CKA_VALUE_LEN in the search template may return objects with values of CKA_VALUE_LEN not matching the search criteria. This defect fix requires that both the corecrypto service and PKCS #11 library be upgraded.
NSE-51232	N/A	C_GetFunctionList now returns the correct Cryptoki version in the CK_VERSION field.
NSE-46095	There is a potential issue when listing a very large number of keys (> 400k keys) which can cause the server to become unresponsive, dependent on system resources. It is recommended that the `limit` and `offset` options be used to process large quantities in smaller batches.	The configuration option `listkeys_max_limit` has been introduced to prevent returning too many keys in a single request. Please refer to the Configuration section of the User Documentation for more information.
NSE-41559	N/A	AES GCM Encryption now behaves correctly for case when the IV argument is omitted. When no IV argument is supplied a random IV will be generated and returned by the HSM.
NSE-49098	N/A	A documentation issue has been resolved regarding the use of HSM protected TLS certificates. Only module protected keys can be used in this manner.
NSE-52641	N/A	The Web Services PKCS#11 Library now returns CKA_ATTRIBUTE_SENSITIVE instead of CKA_ATTRIBUTE_INVALID when used in a template for C_GetAttributeValue with a CKO_SECRET_KEY object.
NSE-52903	N/A	The Web Services PKCS#11 Library now returns CKR_HOST_MEMORY in all cases where memory allocation failed.

Reference	Description in v3.0	Fix in v3.1
NSE-53080	N/A	Fixed an issue where valid DER encoded values for CKA_SUBJECT and CKA_ISSUER would be rejected when creating an X509 certificate object with C_CreateObject.
NSE-53135	N/A	Fixed an issue where migrated certificates had their CKA_SUBJECT and CKA_ISSUER fields encoded incorrectly. It is recommended that certificates migrated from previous versions are removed and migrated again with the DBMT included in this release.

4.1. Known Issues

Reference	Description
NSE-48648	The Web Services PKCS#11 library has a dependency on a third party called `cpprestsdk` which has an internal threadpool limit of 40. There is a potential issue in the PKCS#11 library which means that if an application is running more than 40 threads and encounters a large number of persistent errors from the WSOP `corecrypto` service then the threads can become blocked and an application restart would be necessary. This issue can be mitigated by using fewer threads, and by making use of the config file options `MAXRETRIES` and `RETRYDELAY`. Increasing the value of `RETRYDELAY` introduces a delay between retries of failed WSOP requests.
NSE-52845	When operating close to the active Protection Domain capacity limit, attempts to activate further domains can sometimes be blocked and available capacity in the cache lost. Avoid using small values for the capacity limit and in some cases a restart of corecrypto may be required to release lost cache capacity.
NSE-53106	String fields such as CKA_LABEL and CKA_APPLICATION should not contain any HTML character for example `<`, `>` or `&` as this can result in those values becoming corrupted when they are retrieved later.

Reference	Description
NSE-53579	When using Security World Software v13.3 with Web Service Option Pack 3.1.0, the installation may hang and fail to complete. To overcome this, `/opt/nfast/scripts/startup/wait-for-corecrypto` should be deleted before running the installation script. This will mean that the installation script may incorrectly state that the service has started successfully even if it has not been configured correctly. Please refer to section *Install the Web Services Option Pack* of the User Documentation for more information on verifying a successful WSOP installation.