Web Services Option Pack

# nShield Web Services v3.3.0 Release Notes

12 June 2024

© 2024 Entrust Corporation. All rights reserved.

# Table of Contents

# 1. Introduction

These release notes apply to version 3.3.0 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.

## 1.1. Versions of these Release Notes

| Revision | Date | Description |
|---|---|---|
| 1.0 | 2024-06-10 | Release notes for the nShield Web Services Option Pack v3.3.0 |

# 2. Features of nShield Web Service Option Pack 3.3.0

## 2.1. OpenAPI 3.0.3

The OpenAPI specification used by the Web Services Option Pack has been updated to version 3.0.3.

## 2.2. New HSM protected TLS key config option

A new configuration option `exclude_tls_key` manages the visibility of the HSM protected key used for TLS authentication. By default, the HSM-protected TLS key will be excluded from all Web Services Option Pack operations. For details, see the https://nshielddocs.entrust.com/wsop-docs/v3.3.0/user-guide/configuration.html chapter.

## 2.3. API Gateway support

This release provides new configuration options for operating Web Services Option Pack behind an API Gateway. The service can be configured to support client identifcation via a JWT or custom defined headers. For details, see the https://nshielddocs.entrust.com/wsop-docs/v3.3.0/user-guide/configuration.html chapter.

## 2.4. Support for consistent requests across multiple Web Services Option Pack instances

Many endpoints have been extended to include an optional passphrase for activating the relevant protection domain, if required. For details, see the https://nshielddocs.entrust.com/wsop-docs/v3.3.0/user-guide/rest-api.html chapter.

## 2.5. Extended support for future KeySafe 5 integrations

This release uses a new database schema to allow future KeySafe 5 integrations.

> Users who are upgrading from a previous version of Web Services Option Pack must use the new `migrate-schema` function of the Database Management Tool to update previous database records prior to the installation of the new `corecrypto` service. For details, see the https://nshielddocs.entrust.com/wsop-docs/v3.3.0/user-guide/upgrade.html chapter.

Additionally, a new configuration option has been provided to identify a standalone Web Services Option Pack installation which does not share the database with any other applications. For details, see the https://nshielddocs.entrust.com/wsop-docs/v3.3.0/user-guide/configuration.html chapter.

## 2.6. New Algorithm support

Support for the following signing and verification algorithms has been added:

- `ECDSA-SHA256`
- `ECDSA-SHA384`
- `ECDSA-SHA512`

## 2.7. New PKCS #11 functionality

- Generation of ECDSA keys with `C_GenerateKeyPair`:
    - `CKK_EC` key types generated using `CKM_ECDSA_KEY_PAIR_GEN`
- New ECDSA mechanisms for sign and verify:
    - `CKM_ECDSA_SHA256`
    - `CKM_ECDSA_SHA384`
    - `CKM_ECDSA_SHA512`
- Modification of object attributes with `C_SetAttributeValue`:
    - `CKA_LABEL`
    - `CKA_EXTRACTABLE` (only from `CK_FALSE` to `CK_FALSE`)

## 2.8. nShield Web Services Key Storage Provider

This release introduces the nShield Web Services Key Storage Provider, a web services-based Cryptography API: Next Generation (CNG) provider that can be used to generate and use keys for creating and verifying signatures.

The following set of algorithms are supported for signing operations:

- RSA
- ECDSA_P256
- ECDSA_P384
- ECDSA_P521

The nShield Web Services Key Storage Provider can be used to integrate with the following applications:

- Microsoft Authenticode
- Microsoft Internet Information Services (IIS)
- Microsoft Active Directory Certificate Services (AD CS)

See the *nShield Web Services CNG User Guide* for further information.

# 3. PKCS #11 v3.0 compliance.

This release is compliant with PKCS #11 Version 3.0 (https://docs.oasis-open.org/pkcs11/pkcs11-base/v3.0/os/pkcs11-base-v3.0-os.html).

# 4. Compatibility

## 4.1. Supported MongoDB versions

This release has been tested against MongoDB version 7.0.4.

## 4.2. 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 5s (Base, Mid, High)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield 5c (Base, Mid, High, Serial Console)

## 4.3. 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 and the nShield Web Services Key Storage Provider have been tested for compatibility with the following operating systems:

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

## 4.4. Supported Security World versions

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

- Security World v12.80
- Security World v13.3 or greater

> A minimum version of 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 Web Services Option Pack. See the nShield 12.80 Security World Software release notes for further details.

## 4.5. API version

The nShield Web Service Option Pack REST API version has been increased to v1.5.0.

# 5. Defect Fixes

| Reference | Description in v3.2 | Fix in v3.3 |
|---|---|---|
| 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 Web Services Option Pack server 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 Web Services Option Pack requests. | The Web Services PKCS #11 library has replaced the dependency on cpprestsdk with libcurl. This fixes an issue that could cause an application to hang when running more that 40 threads and encountering persistent errors from the Web Services Option Pack server. |
| 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. | HTML characters saved in string attributes are not corrupted when retrieved. |
| NSE-54022 | The Web Services Option Pack server can temporarily become unresponsive if a large number of time intensive requests are sent concurrently. This will cease when the requests are completed. | New concurrent request limit configuration options have been added to allow Web Services Option Pack to be tuned to the hardware resources. |
| NSE-56651 | An incorrect HTTP response status code of 422 is returned (instead of 400) when a key generation request is rejected because the key ident parameter contains non-alphanumeric characters. | When a key generation request is rejected because the `ident` parameter contains non-alphanumeric characters a correct HTTP response status code of 400 is now returned. |
| NSE-56871 | The `offset` filter option is not supported by the `protectiondomains` endpoint. If needed, `offset` can be used with the `groups` endpoint in order to identify and retrieve the desired protection domain. | The `offset` filter option is now supported by the `protectiondomains` endpoint. |

| Reference | Description in v3.2 | Fix in v3.3 |
|---|---|---|
| NSE-56921 | Web Services Option Pack will not self recover if the connection to the MongoDB server is interrupted enough for the periodic health check to fail. If this happens, the Web Services Option Pack service will need to be restarted before the system can resume operation. | Web Services Option Pack will now recover if the connection to the MongoDB server returns after an unsuccessful health check without the need for a restart. |
| NSE-57190 | When a CRL is processed, invalid certificates can be ignored silently. However, a successfully revoked certificate is reported correctly in the logs. | When a CRL is added to the `crl_directory` that has an invalid signature, an appropriate error is logged. Issues with CRL files are now classified as ERROR level instead of WARNING level in the logs. |
| NSE-57210 | N/A | A documentation issue has been resolved regarding the use of filters when sending a GET request. |
| NSE-57708 | N/A | Updated the help text for `dbmt migrate` so that the required parameters for the `key` option are clearer. |
| NSE-58786 | N/A | Fixed an issue where sending an activate protection domain request with a blank passphrase would return an incorrect error code. |
| NSE-59253 | N/A | Corrected discrepencies in some examples of the API specification file. |
| NSE-60609 | N/A | Fixed an issue where the softcardtool failed to correctly parse configuration files with trailing spaces. |
| NSE-60703 | N/A | Fixed an issue which would allow partial migration of PKCS #11 objects. |
| NSE-60805 | N/A | Fixed an issue which prevented DBMT support for Security World v13.4+. |
| NSE-61433 | N/A | `CKA_PRIVATE` is no longer a required attribute when creating objects or generating keys. When omitted a default value is now used. |

| Reference | Description in v3.2 | Fix in v3.3 |
|---|---|---|
| NSE-61703 | N/A | Fixed a segmentation fault produced when the template for a PKCS #11 object creation contained a string attribute (eg; `CKA_LABEL`) which had NULL pointer as a value. |
| NSE-63134 | N/A | Fixed an issue where the database could not be easily updated after a change in Security World files. The DBMT db-init function can now be used to update these files in the database. |
| NSE-64288 | N/A | Keys with unsupported appnames can no longer be migrated into the database using `dbmt migrate`. Instead of being migrated, these keys will be skipped. |

# 6. Known Issues

| Reference | Description |
|---|---|
| NSE-56623 | Key records from releases prior to Web Services Option Pack version 3.2 may be incompatible with newer releases of Web Services Option Pack and be limited in future functionality. Customers wishing to upgrade from version 3.0 or 3.1 should contact Entrust Support for more information. |
| NSE-62643 | It is not possible to use RSA when performing an integration with the nShield Web Services Key Storage Provider and Microsoft IIS. Attempting to do so will result in the provider returning the following error: `pszAlgId must not be NULL in BCRYPT_PKCS1_PADDING_INFO`. |
| NSE-62766 | Using the nShield Web Services Key Storage Provider to list the keys in a protection domain can result in `ServiceUnavailable` being returned from the `corecrypto` service if the number of keys in the protection domain exceeds 10,000. |
| NSE-62811 | If the system that is hosting the Web Services Option Pack is restarted, the service can fail to automatically restart if the MongoDB server is not reachable in time. In this case the service can be started manually when the database is available. |
| NSE-63105 | If the HSM is put into a non-operational mode, when it is returned to `Operational` mode the `corecrypto` service must be restarted before normal service can resume. |
| NSE-63763 | Descriptions of individual nShield Web Services Key Storage Provider event log entries, when viewed through Event Viewer, may contain text indicating that the description for a particular Event ID cannot be found. This message is benign as the logs generated by the provider are contained within the description.<br>To address this issue, copy `nflog-msgs.dll` from `%ProgramFiles%\nCipher\WebServices\CNG\lib\nflog-msgs.dll` (assumes default install location) to `%ProgramFiles%\nCipher\nfast\bin\nflog-msgs.dll` if it does not already exist. |
| NSE-64343 | There is an issue when using `dbmt db-init` that any OCS must have passphrase recovery disabled (e.g. in `createocs` the `-no-pp-recovery` option needs to be set). |