Web Services Option Pack

nShield Web Services v3.3.1 Release Notes

21 October 2024

Table of Contents

1. Introduction

These release notes apply to version 3.3.1 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	2024-10-21	Release notes for the nShield Web Services Option Pack v3.3.1

2. Features of nShield Web Service Option Pack 3.3.1

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 nShield Security 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 v3.3	Fix in v3.3.1
NSE-60805	N/A	Fixed an issue which prevented the DBMT from being installed with Security World v13.6.3.

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. 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).