Web Services Option Pack

WSOP v3.0.2 Release Notes

10 April 2024

Table of Contents

1. Introduction

These release notes apply to version 3.0.2 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 3.0.2

2.1. Support for MongoDB added

A standalone database management system has been introduced for the storing of non-confidential Security World keys and token data. A database driver that supports MongoDB has been implemented which allows WSOP to access a MongoDB database.

See the *User Guide* for more information.

2.2. New configuration options

New configuration options have been added for:

- New health endpoint functionality.

  The health endpoint can now be configured for different intervals, timeouts, and authentication methods.

- MongoDB settings.

  Additional configuration options for the new database support are available for selecting the DB authentication method, TLS authentication, and enabling Virtual Partitioning support.

See the *User Guide* for more information on these new options.

2.3. New PKCS #11 library

This release provides a new version of the PKCS #11 library that uses WSOP v3.0.2. Custom PKCS #11 endpoints have been added, enabling this library to provide the core functionality of the PKCS #11 API and allows users to create AES keys and perform encryption and decryption using AES CBC Padded and Non-Padded mechanisms. The library also provides functionality to create certificate and data objects. For details, see *PKCS #11* in the *nShield Web Service Option Pack User Guide*.

The PKCS #11 library also uses another library called `libCppRestSwaggerClient.so`

In WSOP 3.0 and later versions, you can use four example programs to obtain information about Softcards:

`ckinfo`	Version of the PKCS#11 library.
`cklist`	Objects created on the Softcard.
`ckmechinfo`	Supported mechanisms.
`softcardtool`	Version of the tool that generated the Softcard. Run these programs with the following commands:

```
/opt/nfast/wsop/pkcs11/bin/ckinfo-dynamic --library /opt/nfast/wsop/pkcs11/lib/libpkcs11wsop.so
/opt/nfast/wsop/pkcs11/bin/ckmechinfo-dynamic --library /opt/nfast/wsop/pkcs11/lib/libpkcs11wsop.so
/opt/nfast/wsop/pkcs11/bin/cklist-dynamic --library /opt/nfast/wsop/pkcs11/lib/libpkcs11wsop.so
/opt/nfast/wsop/pkcs11/bin/softcardtool -g --name=<new-softcard-name>
```

2.4. Virtual Partitioning

Virtual Partitioning is a new option that allows the visibility of the database records to be controlled on a client by client basis. The client's X.509 certficate is used to set the virtual partition view that the client will have.

See the *User Guide* for more information on Virtual Partitioning.

2.5. Database Management Tool

This release introduces the Database Management Tool (DBMT) which is a utility to support the migration of kmdata files into the MongoDB database. The Database Management Tool migration also supports Virtual Partitioning and this can be used to maintain RFS directory partitions of Softcards and Key grouping in the new database.

Entrust recommends that a separate machine be used for the migration. This migration machine must have Security World 12.80+ installed, as well as the DBMT utility, and `kmdata-local` should be set to the directory containing the keys to be migrated.

Migration of PKCS #11 objects is limited to what is supported by the PKCS #11 library included in this release. At this time, only the migration of AES Keys, X.509 Certificates, and Data Objects are supported.

If using Virtual Partitioning, ensure that the segregation database and collection have been populated with each client's X.509 Certificate Subject and Issuer fields along with matching segregation label. The client's X.509 Certificate is used by the DBMT to insert the database records into the correct virtual partition.

An example of a simple migration:

```
dbmt migrate --config <CONFIG> --library <LIBRARY>
```

An example of a migration using Virtual Partitioning:

```
dbmt migrate --config <CONFIG> --library <LIBRARY> --segregate <CERT>
```

where <CERT> is the client's X.509 certificate and <LIBRARY> is the path to the Entrust PKCS #11 library `libcknfast.so`. See the *User Guide* for more information on using the Database Management Tool.

2.6. Create and delete Softcard APIs

New REST APIs are now available for the creation and deletion of Softcards.

Softcard creation is through the `/km/v1/protectiondomains` endpoint with `POST` and the `type` field must be supplied as `Softcard`. The `name` and `passphrase` fields have the standard restrictions.

Example Softcard creation:

```
# Create softcard
curl -k -X POST ${CLIENT1} \
    --header 'Content-Type: application/json' \
    --header 'Accept: application/json' \
     -d '{"name":"softcard1","passphrase":"passphrase1","type":"Softcard"}' \
     'https://127.0.0.1:18001/km/v1/protectiondomains' | jq
{
  "id": "e3307c07-300e-585a-95da-ed4f3d0c226e"
}
```

Softcard deletion is also through the `/km/v1/protectiondomains` endpoint but with `DELETE`.

Example Softcard deletion:

```
# Delete softcard
```

```
curl -k -X DELETE ${CLIENT1} \
  'https://127.0.0.1:18001/km/v1/protectiondomains/025ad489-3ec8-5bbc-b251-f0e497f7cd48?cascade=keys' | jq
```

For further details, see the API section below.

2.7. Additional algorithm support

- Encryption/Decryption Algorithms:
  - A128CBC-NOPAD
  - A192CBC-NOPAD
  - A256CBC-NOPAD

2.8. X.509 Extension Subject Alternative Name

WSOP 3.0 requires that Subject Alternative Name (SAN) extension fields are defined for any X.509 certificates used for TLS authentication.

3. Compatibility

3.1. 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)

3.2. 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
- SUSE Enterprise Linux 12 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 7.6 x64
- Oracle Enterprise Linux 8 x64

3.3. Supported Security World versions

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

- Security World v12.80

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.

3.4. API version

The nShield Web Service Option Pack REST API version has been increased to v1.2.0.

3.5. API additions

The following support has been added to the API:

Crt	Endpoint	Verb	Operation
1	`/km/v1/protectiondomains`	`POST`	Creates a new protection domain. The body must contain a JSON representation of the desired parameters. Will also create a default group for the protection domain.

2	`/km/v1/protectiondomains`
	
	`/km/v1/protectiondomains?cascade=[groups|keys]`
		`DELETE`	Deletes the protection domain.
			
			The cascade query parameter will specify whether deletion should only be allowed when the protection domain is empty (the default), or when it contains (empty) groups or when those groups also contain keys. Deleting the protection domain in this case deletes all contained resources.
			
			The method will return `204 No Content`.

4. Defect Fixes

Reference	Description in v2.1	Fix in v3.0
NSE-32356	When corecrypto serves a request for a WSOP REST API call, it logs a line with information including the endpoint (path) that the client requested, and the HTTP response status that corecrypto sent. In previous releases, HTTP response status 200 is always logged, regardless of the actual status code.	The logging is fixed to log the actual HTTP response status code.
NSE-39635	Health Check HTTP error 503 messages were incorrectly being logged with the INFO category.	These events are now correctly logged with the ERROR category.

4.1. Known Issues

Reference	Description
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.
NSE-48100	Sign and Verification with PS512 when using a 1k RSA key is not supported through WSOP.
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-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.