nShield Database Security Option Pack

nDSOP v2.1.0 Release Notes

10 April 2024

Table of Contents

1. Introduction

These release notes apply to version 2.1.0 of the nShield Database Security Option Pack (nDSOP). They contain information specific to this release such as new features, defect fixes, and known issues.

The release notes may be updated with issues that have come to light after this release has been made available. Please check the https://nshieldsupport.entrust.com/hc/en-us/sections/360001115837-Release-Notes for the most up to date version of this document.

Access to the Support Portal is available to customers under maintenance. Please contact Entrust nShield Technical Support at nshield.support@entrust.com to request an account.

1.1. Purpose of this release

nShield Database Security Option Pack v2.1.0 addresses a number of known issues and introduces a number of enhancements over the previous release, including:

- Support has been added for FIPS 140-2 Level 3 and Common Criteria CMTS Security Worlds.
- It is no longer necessary to restart the provider in order to add or remove modules.
- Keys are automatically loaded on demand.

2. Features of nShield Database Security Option Pack

2.1. Support for fips-140-2-level-3 and common-criteria-cmts Security Worlds

The nShield Database Security Option Pack now supports FIPS 140-2 Level 3 and Common Criteria CMTS Security Worlds (meaning Security Worlds which were created when specifying either `fips-140-2-level-3` or `common-criteria-cmts` as the mode at the point of Security World initialization). See Compatibility for the types of Security World supported.

2.2. Adding and removing modules no longer requires a restart

It is now possible to add and remove modules without restarting the SQLEKM provider. A module is considered available for use by the provider when it is both enrolled in a Security World and is shown as being usable (which can be confirmed by running `nfkminfo`).

2.3. Keys are automatically loaded on demand

Previously, once a session was opened, the list of keys available would remain fixed during the lifetime of the session. This meant that to detect the addition or removal of keys, it was necessary to restart the SQLEKM provider to refresh the key list. It is now possible to add and remove keys without restarting the SQLEKM provider. The existence of a key will automatically be checked at the point of its use, as well as at periodic intervals thereafter. To manually force the removal of keys from the provider at a specific point, the following query will provoke the key list to be refreshed:

```
DECLARE @ProviderId int;
SET @ProviderId = (SELECT TOP(1) provider_id
FROM sys.dm_cryptographic_provider_properties
WHERE friendly_name LIKE 'nCipher SQLEKM Provider');
SELECT * FROM sys.dm_cryptographic_provider_keys(@ProviderId);
GO
```

3. Compatibility

3.1. Supported Enterprise Editions of Microsoft SQL Server

The following Enterprise Editions of Microsoft SQL Server are supported by this release:

- Microsoft SQL Server 2019 x64
- Microsoft SQL Server 2017 x64
- Microsoft SQL Server 2016 x64

We recommend that all the latest service packs, updates and hotfixes for your version of Microsoft SQL Server are installed.

3.2. Supported Hardware Security Modules (HSMs)

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

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

3.3. Supported operating systems

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

- Microsoft Windows Server 2019 x64
- Microsoft Windows Server 2016 x64

3.4. Supported versions of Security World software

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

- Security World v12.60 (supporting FIPS 140-2 level 2, FIPS 140-2 level 3 and Common Criteria CMTS Security Worlds)
- Security World v12.40.2 (supporting FIPS 140-2 level 2 and FIPS 140-2 level 3 Security Worlds)

Firmware versions supported by the above releases are also supported by nDSOP.

4. Upgrading v1.01.00 deployments

The steps necessary to upgrade from an existing v1.01.00 deployment are detailed in the *nShield Database Security Option Pack User Guide*.

If upgrading from an existing nDSOP v1.01.00 deployment, and the use of v12.40.2 Security World software is retained, it will be necessary to invoke `sqlekm_retarget_keys` as follows:

```
"%NFAST_HOME%\python\bin\python.exe"
"%NFAST_HOME%\python\scripts\sqlekm_retarget_keys.py"
```