nShield Monitor

Monitor v3.1.0 Release Notes

8 April 2024

Table of Contents

1. Introduction

nShield® Monitor is an Entrust nShield® HSM monitoring solution. It is delivered as a virtual appliance (OVA format) to operate in a VMware virtualization environment, as a Hyper-V image to operate in the Microsoft Hypervisor environment, and as a Docker container.

These release notes apply to version 3.1.0 of nShield Monitor. They contain information specific to this release such as new features, defect fixes, and known issues.

This document may be updated with issues that have become known after this release has been made available. Check https://nshieldsupport.entrust.com/hc/en-us/sections/360001115837-Release-Notes for the most up to date version of this document and the nShield Monitor user documentation.

Access to the Entrust nShield Help Center is available to customers under maintenance. Contact Entrust nShield Technical Support at nshield.support@entrust.com to request an account.

2. Purpose of this release

nShield Monitor version 3.1.0 addresses a number of known issues and introduces a number of enhancements over the previous release, including:

- The ability to recognise and monitor the nShield Connect CLX, nShield 5s and nShield 5c hardware security module (HSM) variants.
- Increases the number of groups supported.
- Latest security updates.

3. Changes in this release

The nShield Monitor version 3.1.0 release introduces a number of enhancements. These are discussed in the following sections.

3.1. Updated HSM monitoring support

nShield Monitor now recognises, and supports, the monitoring of the nShield Connect CLX, nShield 5s and nShield 5c hardware security module (HSM) variants.

3.2. Increased number of groups

The number of groups which could previously be created was limited to 32. This limit has been increased to 128.

3.3. User documentation

The nShield Monitor user documentation is no longer available via the nShield Monitor UI.

- Release notes and user documentation for recent releases are publicly available at https://nshielddocs.entrust.com.
- PDF versions of all supported release notes and user documents are available in the Entrust nShield Help Center at https://nshieldsupport.entrust.com/hc/en-us/categories/360000473317-Documents-Manuals. Access to the Entrust nShield Help Center is available to customers under maintenance. Contact Entrust nShield Technical Support at nshield.support@entrust.com to request an account.

4. Defect fixes

The following table lists the defects fixed with this release.

Reference	Description
NSE-51334	nShield Monitor shows nShield Connect CLX, nShield 5s and nShield 5c as Edge devices
NSE-56851	Client Host Unreachable by nShield Monitor, even though SNMP commands work as expected

5. Known issues

Reference	Description
NM-806	When the container starts, the following message might appear when running `docker logs`: *Could not convert 0x263b from UCS-2 to a multibyte character: Invalid or incomplete multibyte or wide character* These messages are benign and do not impact the operation of nShield Monitor.
NSE-56490	Recent browser updates to Chrome and Edge have broken some of the UI screen elements.
NSE-57151	nShield Monitor does not distinguish a Connect CLX from a Connect.

6. Upgrading from previous releases

To use nShield Monitor version 3.1.0 either:

- Load a new instance of nShield Monitor
- Use the upgrade `.cmf` file to upgrade an existing nShield Monitor installation

If upgrading from any version before v2.5.5, you must first upgrade to v2.5.5 before upgrading to version 3.1.0. We recommend taking a backup before upgrading, see the *nShield Monitor Installation and User Guide* for further information.

From version 2.5.5, nShield Monitor only supports the monitoring of nShield HSMs. Only nShield Monitor upgrade files are supported.

Contact Entrust nShield Support for further information.

7. Compatibility

nShield Monitor is provided as a CMF to upgrade images in Open Virtual Appliance (OVA) format, Microsoft Hyper-V format and Docker containers.

The OVA / Hyper-V / docker container images include a 64-bit Linux based OS and OVT.

For the latest information on compatibility and system requirements, see the *nShield Monitor Installation and User Guide*.

7.1. Hypervisor compatibility

The OVA can be installed on the following virtual platforms:

- vSphere ESXi 6.5
- vSphere ESXi 6.7
- vSphere ESXi 7.0
- VMware Workstation 12
- VMware Workstation 14
- VMware Fusion 10
- Oracle VirtualBox 6.0

The Hyper-V image can be installed on the following virtual platforms:

- Microsoft Hyper-V
- Microsoft Azure

The Docker container can be deployed on either a physical machine or a virtualization platform which has hardware virtualization support enabled (VT-x or AMD-V).

7.2. Host server requirements

The host server should meet the following requirements:

- 64-bit host OS
- CPU: 2 core 2.0GHz multicore CPU (can be increased as needed)
- Memory: 8GB dedicated memory for nShield Monitor (can be increased)
- Network: Single network attached interface to bridged or physical network
- Disc space to download:

    - An OVA image (1.1 GB)
    - A Hyper-V image (3.3 GB)
    - A Docker container and its associated volumes (1.5 GB)
- Size on the hard drive:
    - 2.3 GB (OVA) / 3.3 GB (Hyper-V) / 1.5 GB (Docker container) (thin provisioned)
    - 326.0 GB (OVA) (thick provisioned)

7.3. nShield compatibility

nShield Monitor is compatible with the following nShield HSM models and software versions:

- nShield Edge, nShield Solo+, nShield Solo XC, nShield Connect+, nShield Connect XC, nShield Connect CLX, nShield 5s and nShield 5c with Security World software v12.40 and higher.