



ENTRUST

nShield Monitor

Monitor v3.0.0 Release Notes

8 April 2024

Table of Contents

1. Introduction	1
2. Purpose of this release.....	2
3. Changes in this release.....	3
3.1. Deployment of nShield Monitor as a Docker container	3
4. Defect fixes	4
5. Known issues	5
6. Upgrading from previous releases.....	6
7. Compatibility	7
7.1. Hypervisor compatibility	7
7.2. Host server requirements	7
7.3. nShield compatibility	8

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 3.0.0 of nShield Monitor. They contain information specific to this release such as new features, defect fixes, and known issues.

The Release Notes may occasionally be updated with issues that have come to light after this release has been made available. Please check Entrust nShield Support at <https://nshieldsupport.entrust.com> for the most up to date version of this document and the nShield Monitor user documentation.

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

2. Purpose of this release

nShield Monitor version 3.0.0 addresses a number of known issues and introduces a number of enhancements over the previous release, including:

- Deployment of nShield Monitor as a Docker container.
- Latest security updates.

3. Changes in this release

The nShield Monitor 3.0.0 release introduces a number of enhancements. These are discussed in the following sections.

3.1. Deployment of nShield Monitor as a Docker container

nShield Monitor can now be deployed as a Docker container on hosts that support hardware virtualization. See the *nShield Monitor Installation and User Guide* for further information.

4. Defect fixes

The following table lists the defects fixed with this release.

Reference	Description
NM-975	Port 465 omitted from SMTP firewall rules and docker configuration.

5. Known issues

Reference	Description
NM-806	When the container starts, the following message might appear when running <code>docker logs</code> : <i>Could not convert 0x263b from UCS-2 to a multibyte character: Invalid or incomplete multibyte or wide character</i> These messages are benign and do not impact the operation of nShield Monitor.

6. Upgrading from previous releases

To use nShield Monitor 3.0.0 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 3.0.0. 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, Solo+, Solo XC, Connect+ and Connect XC with Security World software v12.40 and higher.