nShield Monitor

Monitor v2.8.0 Release Notes

9 April 2024

Table of Contents

1. Introduction

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

These release notes apply to version 2.8.0 of nShield Monitor. They contain information specific to this release such as new features, defect fixes, and known issues.

The Release Notes may vary from time to time, be updated with issues that have come to light after this release has been made available. Please check the nCipher Security Help Centre at https://help.ncipher.com for the most up to date version of this document.

Access to the Support Portal is available to customers under maintenance. Please contact nCipher Security at support@ncipher.com to request an account.

1.1. Purpose of this release

This release delivers an nShield Monitor version 2.8.0 as a CMF upgrade file for environments being upgraded from nShield Monitor version 2.7.0 to nShield Monitor version 2.8.0.

This release of nShield Monitor adds support for SNMP v3 trapsink functionality.

2. Main Features of v2.8.0

2.1. New Features

Reference	Description
NM-577	Add SNMP v3 authentication to SNMP trapsinks

2.2. Defect Fixes

Reference	Description
NM-697	Auto- Logout functionality is not working when it is set while creating or updating the users
NM-699	Password enforcement of <n> length should be allowed to all existing user whenever the password length policy is changed.
NM-622	SNMP trap notification displayed for all the groups , irrespective of group trap setting.
NM-604	Thales references in the MIB should be removed once downloaded.

3. Upgrading from previous releases

To use nShield Monitor v2.8.0:

Use the upgrade `.cmf` file to upgrade an existing nShield Monitor installation

> ℹ️ If upgrading from any version before v2.5.5, you must first upgrade to v2.5.5 before upgrading to version v2.8.0.

> ⚠️ Upgrading to this version of nShield Monitor v2.8.0 will disable further upgrades using CipherTrust update files.

> ⚠️ nShield Monitor eliminates monitoring of payShield devices and only monitors nShield HSMs. Upgrading to nShield Monitor will remove all payShield information.

Contact nCipher support for further information.

4. Compatibility

nShield Monitor is provided in Open Virtual Appliance (OVA) format and the Microsoft Hyper-V format. The OVA / Hyper-V image includes 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*.

4.1. Hypervisor compatibility

The OVA can be installed on the following virtual platforms:

- vSphere ESXi 6.0
- vSphere ESXi 6.5
- 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

4.2. 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 size to sufficiently accommodate a minimum OVA Download size of 1.1 GB or Hyper-V image size of 3.3 GB. Size on disc:
    - 2.3 GB (OVA) / 3.3 GB (Hyper-V) (thin provisioned)
    - 326.0 GB (OVA) (thick provisioned)

4.3. 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.