nShield Monitor

Monitor v2.9.0 Release Notes

9 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, and as a Hyper-V image to operate in the Microsoft Hypervisor Environment.

These release notes apply to version 2.9.0 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 Entrust nShield Support at https://nshieldsupport.entrust.com 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 Support at nshield.support@entrust.com to request an account.

1.1. Purpose of this release

This release delivers an nShield Monitor version 2.9.0 as both OVA, Hyper-V and as a CMF upgrade file for environments being upgraded from nShield Monitor version 2.7.0 and later to nShield Monitor version 2.9.0.

This release of nShield Monitor adds support for SNMP v3 trapsink functionality, the ability to integrate with LDAP login service with Active Directory, and branding changes.

2. Main Features of v2.9.0

2.1. Integration with Active Directory and LDAP

nShield Monitor 2.9 can now integrate with Active directory using LDAP Authentication services. Once the basic setup has occurred there is a new page when logged in as an Administrator to connect to the LDAP server. If you select the option to use the LDAP integration, then you will only be able to manage users for nShield Monitor through the standard MS AD/LDAP standard interface outside of nShield Monitor. This feature is enabled either as an OVA or via an upgrade.

2.2. Update nShield Monitor to Entrust Branding

nShield Monitor has been updated to Entrust branding, this does not affect the end user license and there is no change.

2.3. SNMP v3 authentication to SNMP trapsinks

Release 2.9 is provided as the Standard OVA and Hyper-V system. This is the first release where the new V3 Trapsink will be available without having to install an earlier version of nShield Monitor prior to 2.8, which was only delivered as an upgrade file.

Now when selecting SNMPv3 Authentication you can select SHA2 hashing. This requires the latest nCSNMP agent 12.80.

3. Defect fixes

Reference	Description
NM-802	Security updates to JQuery.
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-849	nShield Monitor must send email notification to correct group only.

4. Known issues

Reference	Description
NM-806	Cleartext email SMTP forgot password subject to man in the middle attack. ℹ To mitigate this issue please configure nShield Monitor to use secure port for emails.

5. Upgrading from previous releases

To use nShield Monitor v2.9.0 either:

- Load a new instance of the nShield Monitor v2.6.6 OVA
- 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 v2.9.0.

> Upgrading to this version of nShield Monitor v2.9.0 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 Entrust nShield Support for further information.

6. Compatibility

nShield Monitor is provided as a CMF to upgrade images 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*.

6.1. 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

6.2. 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)

6.3. 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.