nShield Monitor

Monitor v2.9.8 Release Notes

8 April 2024

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
2. Purpose of this release . . . 2
3. Changes in this release . . . 3
    3.1. CSRF (Cross-Site Request Forgery) prevention . . . 3
    3.2. User creation emails use password reset links . . . 3
    3.3. Documentation clarity on configuring secure LDAP . . . 3
    3.4. Updated vSphere ESXi support . . . 3
4. Upgrading from previous releases . . . 4
5. Compatibility . . . 5
    5.1. Hypervisor compatibility . . . 5
    5.2. Host server requirements . . . 5
    5.3. nShield compatibility . . . 6

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 2.9.8 of nShield Monitor. They contain information spe cific 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://trustedcare.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 2.9.8 addresses a number of known issues and introduces a number of enhancements over the previous release, including:

- CSRF (Cross-Site Request Forgery) prevention.
- User creation emails use password reset links.
- Documentation clarity on configuring secure LDAP.
- Updated vSphere ESXi support.
- Latest security updates.

3. Changes in this release

The nShield Monitor 2.9.8 release introduces a number of enhancements. These are discussed in the following sections.

3.1. CSRF (Cross-Site Request Forgery) prevention

CSRF tokens are now sent with all requests. If the CSRF token fails to verify e.g. it is absent, or has been tampered with, the request is rejected and an error is returned.

3.2. User creation emails use password reset links

Previously, when an nShield Monitor user was created, a one-time password was emailed to the user and also displayed to the administrator who created the user. nShield Monitor now emails a password reset link to the user when the account is created so that users can set their own passwords. The reset link expires after 60 minutes.

3.3. Documentation clarity on configuring secure LDAP

The *nShield Monitor Installation and User Guide* now provides additional information on how to configure secure LDAP.

3.4. Updated vSphere ESXi support

nShield Monitor now supports vSphere ESXi 6.7 and 7.0. Support for vSphere ESXi 6.0 has been deprecated.

4. Upgrading from previous releases

To use nShield Monitor 2.9.8 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 2.9.8. 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.

5. 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*.

5.1. 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

5.2. 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)

5.3. 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.