KeySafe 5

KeySafe 5 v1.3 Release Notes

24 June 2024

Table of Contents

1. Introduction

These release notes apply to version 1.3 of the nShield KeySafe 5 for Security World. They contain information specific to this release, such as new features, defect fixes, and known issues.

The release notes might be updated with issues that have been discovered after this release has been made available. Check the Support Portal for the most up to date version of this document.

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

1.1. Purpose of this release

KeySafe 5 v1.3 provides a centralized means to securely manage a distributed nShield HSM estate. This release extends the functionality released in v1.2, adding nShield 5s upgrade management functionality, nShield Key listing and Key management data persistence improvements.

This release provides the option to deploy KeySafe 5 as a single binary application.

The *KeySafe 5 Installation and Upgrade Guide* provides details of how to install, upgrade and use the platform. Read this document before installing the platform.

1.2. Versions of these Release Notes

Revision	Date	Description
1.1	2024-06-24	Website link fixes, no content changes to KeySafe 5 v1.3
1.0	2024-06-07	Release notes for KeySafe 5 v1.3

2. Features of nShield KeySafe 5 v1.3

The following sections in these release notes detail the specific key features of the 1.3 version of nShield KeySafe 5.

2.1. nShield KeySafe 5 Local Deployment (single binary install)

KeySafe 5 v1.3 is now provided in a single binary executable format to enable use of KeySafe 5 to manage a single nShield Security World host machine and attached HSMs.

The nShield KeySafe 5 Local Deployment installs alongside the nShield Security World software.

Please see the *KeySafe 5 Installation and Upgrade Guide* for more information.

2.2. nShield 5s Upgrade and VSN Management

KeySafe 5 v1.3 provides the following nShield 5s Upgrade and VSN management operations:

- Storage, listing and deletion of nShield 5s firmware and uboot upgrade images
- Visibility of the nShield 5s Min VSN setting
- nShield 5s firmware and uboot version upgrade
- nShield 5s Min VSN setting changes

Please see the *nShield Security World v13 product documentation* for more information regarding nShield 5s upgrade and Min VSN functionality.

2.3. Key Visibility

KeySafe 5 v1.3 extends the Security World management operations to provide the following:

- Listing of kmdata key files, referred to as "Secrets" in KeySafe 5
- Ability to reveal metadata of Secrets such as key type, length, curve and permissions

Secret deletion is not currently supported.

> Synchronization of a large amount of kmdata key files may take an extended period of time to complete.

2.4. Key Management Data Persistence Improvements

KeySafe 5 v1.3 has improved how it handles Key Management Data persistence such that:

- Local deletion of a resource (Card Set or Softcard) does not result in KeySafe 5 re-syncing the file
- Resources (Card Set or Softcard) created on an nShield host machine are not automatically available to nShield Web Services clients
- Resources (Card Set or Softcard) created via KeySafe 5 are not automatically available to nShield Web Services clients
- nShield Web Services created Softcards are not automatically synced to all nShield host machines

2.5. User Interface Improvements

KeySafe 5 v1.3 provides the following User Interface improvements:

- Overall redesign to improve usability
- Performance and responsiveness improvements

3. Important information

Before deploying KeySafe 5 v1.3, consider the following points.

3.1. nShield KeySafe 5 agent

nShield KeySafe 5 v1.3 requires that all agents are upgraded to v1.3. Differing versions between the central platform and agent is not supported.

3.2. Key Management Data Synchronization

KeySafe 5 takes ownership over certain kmdata synchronization (world, module certs, Card Sets and Softcards), and as such might conflict with existing methods.

Since KeySafe 5 v1.3 if a Card Set or Softcard is removed locally on an nShield Security World host machine, it will no longer be re-synced to that host machine by KeySafe 5.

If there is clock skew between hosts being managed by KeySafe 5 and the central platform then the behaviour of the kmdata synchronization will be impacted. KeySafe 5 Host Management will highlight issues of clock skew in the health of a Host resource.

3.3. nShield Edge

KeySafe 5 can not change the mode of an nShield Edge HSM. For HSM Pools that contains an nShield Edge, you must manually set the HSM mode when creating/loading Security Worlds. For further details, see Known issues from earlier nShield KeySafe 5 releases.

3.4. Remote Administration Authorized Card List

In local management of nShield Security World software the use of nShield Remote Administration smart cards is controlled by an Authorized Card List located at `%NFAST_KMDATA%\config\cardlist`. In this release of KeySafe 5, no restrictions are enforced on which smart cards may be presented to HSMs via KeySafe 5, regardless of the contents of any existing cardlist files.

4. Upgrade information

Before upgrading to KeySafe 5 v1.3, consider the following points.

Information regarding these changes can be found in the *nShield KeySafe 5 v1.3 product documentation*.

4.1. nShield KeySafe 5 agent config file

nShield KeySafe 5 v1.3 agent config file values have changed. KeySafe 5 will attempt to automatically update these values during start-up. A copy of the previous config file will be made.

5. Centralized platform compatibility

5.1. Supported Kubernetes version

This release has been tested on the following Kubernetes versions:

- 1.29

5.2. Supported Istio version

This release has been tested using the following Istio versions:

- 1.21

5.3. Supported external services

This release has been tested using the following external service versions:

Software	Minimum Version	Tested Version
MongoDB	6.0	6.0.14
	7.0	7.0.7
RabbitMQ	3.0	3.12.13

6. KeySafe 5 agent compatibility

6.1. Supported hardware

This release targets deployments with any combination of the following nShield HSMs:

- nShield 5s (Base, Mid, High)
- nShield Solo XC (Base, Mid, High)
- nShield Solo PCI Express (500+, and 6000+)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield Connect CLX (Base, Mid, High)
- nShield 5c (Base, Mid, High)
- nShield Edge

6.2. Supported operating systems

This release has been tested for compatibility with the following operating systems:

- Microsoft Windows Server 2016 x64
- Microsoft Windows Server 2019 x64
- Microsoft Windows Server 2022 x64
- Microsoft Windows Server 2022 Core x64
- Microsoft Windows 10 x64
- Microsoft Windows 11 x64
- Red Hat Enterprise Linux 7 x64
- Red Hat Enterprise Linux 8 x64
- Red Hat Enterprise Linux 9 x64
- SUSE Enterprise Linux 12 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 7 x64
- Oracle Enterprise Linux 8 x64
- Oracle Enterprise Linux 9 x64

For further details on supported hardware and platform combinations, refer to the *nShield Security World software release notes*.

6.3. Supported Security World versions

This release is compatible with the following nShield Security World software installations:

- Security World v12.80
- Security World v13.4
- Security World v13.6

Firmware versions supported by the listed releases are also supported by KeySafe 5 v1.3. For further details on Security World and firmware support, refer to the *nShield Security World software release notes*.

7. KeySafe 5 Local compatibility

7.1. Supported hardware

This release targets deployments with any combination of the following nShield HSMs:

- nShield 5s (Base, Mid, High)
- nShield Solo XC (Base, Mid, High)
- nShield Solo PCI Express (500+, and 6000+)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield Connect CLX (Base, Mid, High)
- nShield 5c (Base, Mid, High)
- nShield Edge

7.2. Supported operating systems

This release has been tested for compatibility with the following operating systems:

- Microsoft Windows Server 2019 x64
- Microsoft Windows Server 2022 x64
- Microsoft Windows 10 x64
- Microsoft Windows 11 x64
- Red Hat Enterprise Linux 8 x64
- Red Hat Enterprise Linux 9 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 8 x64
- Oracle Enterprise Linux 9 x64

For further details on supported hardware and platform combinations, refer to the *nShield Security World software release notes*.

7.3. Supported Security World versions

This release is compatible with the following nShield Security World software installations:

- Security World v13.6

Firmware versions supported by the listed releases are also supported by KeySafe 5 v1.3. For further details on Security World and firmware support, refer to the *nShield Security World software release notes*.

8. Supported identity providers

This release has been tested against the following identity providers:

- Entrust Identity as a Service v5.33
- Microsoft Server 2019 AD FS

> ℹ Other OIDC and OAuth 2.0 providers might be supported.

9. KeySafe 5 deployment script compatibility

9.1. Supported operating systems

The KeySafe 5 deployment script has been tested for compatibility with the following operating systems:

- Red Hat Enterprise Linux 8 x64

9.2. Supported versions of software

The KeySafe 5 deployment script has been tested for compatibility with the following versions of support software:

- OpenSSL 1.1.1s
- OpenSSL 3.0.7
- Podman 3.4.7
- Docker 20.10.19

> Versions of OpenSSL below 1.1.1 are not supported.

10. Issues fixed in nShield KeySafe 5 v1.3

Reference	Description
NSE-57165	The Estate Overview widgets omit values in the legend once the number of unique values is greater than 4.
NSE-57227	Long CodeSafe 5 certificate serial numbers cause overlapping in the KeySafe 5 UI.
NSE-57294	Uploading a CodeSafe 5 Certificate to a certificate resource which has been synced causes the KeySafe 5 UI to render unsuccessfully.
NSE-57305	The CodeSafe 5 Machine configuration toggles revert to disabled state when the dialogue is opened.
NSE-61467	v13 Security World installations remove write permission to the KeySafe 5 Log file

11. Known issues in nShield KeySafe 5 v1.3

See also Known issues from earlier nShield KeySafe 5 releases.

Reference	Description
NSE-62577	The KeySafe 5 UI incorrectly provides an option to disable static module features.
NSE-62874	If an error occurs during a Min-VSN update the HSM mode is not reverted to its original value. Users are advised to manually perform the HSM mode change via KeySafe 5.

12. Known issues from earlier nShield KeySafe 5 releases

These issues are still present in v1.3.

Reference	Description
NSE-37786	When creating/loading/unloading a Security World on an HSM Pool that contains an nShield Edge HSM, you must manually change the mode of the nShield Edge to Initialization before sending the request. You should also ensure the HTTP server write timeout in the keysafe5-backend Helm chart is configured to a value that exceeds the time expected to write/read a card on an nShield Edge.
NSE-46785	On Windows machines, any kmdata file created by the nShield KeySafe 5 agent service (for example, a softcard created by KeySafe 5) will not automatically have file permissions to be modified by non-Administrator user accounts. This means when a local Windows user tries to do an action that wants to overwrite that kmdata file (such as locally changing a softcard passphrase) they will not have permission to rewrite the file in kmdata. The workaround is for an Administrator user to manually modify the permissions on the kmdata files created by keysafe5-agent to allow local users to modify them.
NSE-51100	KeySafe 5 does not enforce the Remote Administration authorized card list. Further information can be found in the Release Notes
NSE-51114	When running the deploy.sh script with DOCKER_REGISTRY set, Docker images can not be pulled from an authenticated Docker registry. The workaround is to not set DOCKER_REGISTRY and the deploy script will spin up its own registry for use.
NSE-52265	KeySafe 5 can not disable SEE Activation (Restricted) unless all hosts in the HSM Pool are healthy at the time of the disable action. The workaround is to manually remove the feature enablement certificate files from the host machine.
NSE-56419	KeySafe 5 allows the creation of an SP800-56Ar3 Securirty World using v1.0 Java cards. Security World creation will complete, but the ACS will be unusable for future operations. Ensure use of v1.1 Java cards prior to creating a Security World with SP800-56Ar3 enabled.

Reference	Description
NSE-56722	The FPUI on an nShield 5c does not accurately reflect the HSM mode and the mode banner is not displayed when the HSM mode is changed via KeySafe 5.
NSE-57196	Deletion of a Security World via KeySafe 5 will not persist in the case where a KeySafe 5 agent is enabled on an nShield 5c and that nShield 5c has had world kmdata files synced. The workaround is to ensure that the nShield 5c kmdata is deleted prior to removing from KeySafe 5.