KeySafe 5

KeySafe 5 v1.2 Release Notes

8 April 2024

Table of Contents

1. Introduction

These release notes apply to version 1.2 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 v1.2 provides a centralized means to securely manage a distributed nShield HSM estate. This release extends the functionality released in v1.1, adding CodeSafe 5 management functionality and FIPS 140 updates.

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

1.2. Versions of these Release Notes

Revision	Date	Description
1.2	2024-01-18	No software changes. New version of the Release Notes accompanies an online-only document set release that fixed rendering problems in the HTML and PDF.
1.1	2023-12-12	Addition of the OVA Package Information section
1.0	2023-08-22	Release notes for the release of KeySafe 5 v1.2

2. Features of nShield KeySafe 5 v1.2

The following sections in these release notes detail the specific key features of the 1.2 version of nShield KeySafe 5.

2.1. nShield KeySafe 5 agent on an nShield 5c

The nShield 5c image released in nShield Security World v13.4 ships with a KeySafe 5 agent which can be configured to provide updates and management functionality direct to the nShield KeySafe 5 central platform.

This provides the following:

- CodeSafe 5 management
- Direct health reporting of the health of a remote HSM
- Limited device management prior to enrolling the module with a host machine

> ❗ The nShield KeySafe 5 agent on an nShield 5c must be configured for nShield KeySafe 5 to manage the CodeSafe 5 environment on the nShield 5c. This is in addition to the nShield 5c being enrolled with a hardserver running on a host machine with the nShield KeySafe 5 agent running.

Please see the *nShield KeySafe 5 v1.2 product documentation* and *nShield Security World v13.4 product documentation* for more information.

2.2. nShield CodeSafe 5 management

KeySafe 5 v1.2 provides the following CodeSafe 5 Management operations:

- Storage, listing and deletion of CodeSafe 5 images
- Storage, listing and deletion of CodeSafe 5 certificates
- Loading, control, configuration and unloading of CodeSafe 5 images to Pools of HSMs
- Loading and unloading of CodeSafe 5 certificates to Pools of HSMs
- Management of deployed CodeSafe 5 images, including setting the auto start property, SSH daemon configuration and log management.

Please see the *nShield Security World v13.4 product documentation* for more information regarding nShield CodeSafe 5.

2.3. FIPS 140 updates

2.3.1. FIPS 140 SP800-56Ar3

FIPS 140 Implementation Guidance D.1 mandates adoption of the SP800-56Ar3 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf) rules. The v12.72 firmware introduced new restrictions to the strict-FIPS mode to reflect these new rules. These restrictions apply to all subsequent versions of firmware.

This change impacts the FIPS level 3 v3 (DLf3072s256mAEScSP800131Ar1) Security World modes (either newly created v3 worlds or v3 security worlds created with previous releases) loaded into the updated v12.72 firmware with the compliance mode enabled.

For more details please see the *nShield Security World v12.72 release notes*.

KeySafe 5 v1.2 introduces support for enabling this compliance mode when creating or loading the Security World.

> ❗ Use of this compliance mode has implications on the Remote Administration Cards. See the *nShield Security World v12.72 release notes* for more information.

2.3.2. Security World Mode enum updates

In previous KeySafe 5 releases the Security World FIPS Level-3 mode was called `fips-140-2-level-3`, which reflected the FIPS 140-2 compliance of that Security World. With the introduction of the nShield 5s which now complies with FIPS 140-3, this Security World mode has been renamed to `fips-140-level-3`.

This mirrors the change in nShield Security World v13.3. See the *nShield Security World v13.3 release notes* for more information.

The updated enum values used for Security World reporting and creation are as follows:

Added values:

- `unrestricted`
- `fips-140-level-3`

Deprecated values:

- `fips-140-2-level-2` is deprecated and maps to `unrestricted` for Security World Creation requests
- `fips-140-2-level-3` is deprecated and maps to `fips-140-level-3` for Security World Creation requests
- `legacy-fips-140-2-level-2` is deprecated
- `legacy-fips-140-2-level-3` is deprecated

3. Important information

Before deploying KeySafe 5 v1.2, consider the following points.

3.1. nShield KeySafe 5 agent

nShield KeySafe 5 v1.2 requires that all agents are upgraded to v1.2. 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.

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.

3.5. OVA Package Information

The packaging of an earlier release of KeySafe 5 v1.2 was malformed which prevented OVA installs over a hosted URL in some instances of VMWare ESXi.

The malformed packaging is identified by the contents of the `version.txt` file in the package root containing `1.2.0-f4b80015`.

A new package has been released, identifiable by the contents of `version.txt` being `1.2.0-3a9ba698`. Entrust recommends that all future OVA installs of KeySafe 5 v1.2 use this package.

Please note that the installed product is not impacted, as such existing instances of KeySafe 5 v1.2 are not required to be upgraded.

4. Upgrade information

Before upgrading to KeySafe 5 v1.2, consider the following points.

Information regarding these changes can be found in the *nShield KeySafe 5 v1.2 product documentation*.

4.1. nShield KeySafe 5 agent AMQP authentication

nShield KeySafe 5 v1.2 requires that the username used for AMQP authentication contains the hostname that the KeySafe 5 agent identifies as.

A new binary, `amqptls` is included with the KeySafe 5 agent installer to facilitate generation of a private key and CSR to ease this process.

4.2. nShield KeySafe 5 OVA AMQP vhost change

nShield KeySafe 5 v1.2 makes the default AMQP connection vhost value consistent across all install methods.

For existing nShield KeySafe 5 OVA deployments, this requires a KeySafe 5 agent configuration file update to include the `nshieldvhost` value in the AMQP URL.

5. Centralized platform compatibility

5.1. Supported Kubernetes version

This release has been tested on the following Kubernetes versions:

- 1.27

5.2. Supported Istio version

This release has been tested using the following Istio versions:

- 1.17

5.3. Supported external services

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

Software	Minimum Version	Tested Version
MongoDB	4.4	5.0.19
RabbitMQ	3.0	3.11.19

6. Hypervisor compatibility

The OVA can be installed on the following virtual platforms:

- VMWare ESXi 6.7
- VMWare ESXi 7.0
- KVM Hypervisor (Red Hat 7.8 and above)
- Oracle VirtualBox
- VMWare Fusion 12

7. KeySafe 5 agent 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 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

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 v12.80
- Security World v13.3
- Security World v13.4

Firmware versions supported by the listed releases are also supported by KeySafe 5 v1.2. 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 v5.30
- 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

> ℹ Versions of OpenSSL below 1.1.1 are not supported.

10. Issues fixed in nShield KeySafe 5 v1.2

Reference	Description
NSE-46050	KeySafe 5 does not support creation of an SP800-56Ar3 compliant Security World.
NSE-46197	Tabbing between a 'passphrase' text box and a 'passphrase confirmation' text box in the KeySafe 5 UI moves the cursor to the 'show passphrase' icon, not the next text box. Pressing enter/return after entering a password does not click confirm.
NSE-50294	KeySafe 5 deploy script dry run erroneously reports that it will install istio when it is already installed.
NSE-51279	During bulk enablement of feature certificates, no option is provided to clear the module(s).
NSE-51706	Occasionally an Uncaught error appears in the browser console when navigating the KeySafe 5 UI. This is harmless and can be ignored.
NSE-51708	On some pages in the KeySafe 5 UI 400 and 404 errors appear in the browser console. These are harmless and can be ignored.
NSE-51791	KeySafe 5 Agent runs with excessive privilege on Windows
NSE-52091	Screen flickering can occur on the 'Security World' tab on the Pool information page when no Security World has been loaded to that Pool.
NSE-52111	Documented upgrade steps incorrectly lowercase the 'pullPolicy' 'always' value, the correct casing is 'Always'.
NSE-52119	Requesting a negative timeout is incorrectly available as an option when creating a CardSet in the KeySafe 5 UI. Proceeding with the request will cause an error to be returned.
NSE-52189	When loading a Security World on the Pool information page, the selected Security World can be deselected by a background fetch action. Depending on the 'pollInterval' values used when installing the KeySafe 5 UI, this can make it impossible to load a Security World via this dialogue.
NSE-52237	Deletion of a Security World is prevented if a Pool it is loaded on is deleted before deallocating the Pool.
NSE-53623	Feature cert upload dialogue allows the user to move next without providing a file.
NSE-55415	KeySafe 5 backend API returns wrong status code when attempting to set an invalid passphrase.
NSE-56706	Changing OS time on the KeySafe 5 Central Platform causes a CrashLoopBackOff.

11. Known issues in nShield KeySafe 5 v1.2

See also Known issues from earlier nShield KeySafe 5 releases.

Reference	Description
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.
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-57165	The Estate Overview widgets omit values in the legend once the number of unique values is greater than 4.
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.
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. The upload succeeds, and the user is advised to refresh their browser window.
NSE-57305	The CodeSafe 5 Machine configuration toggles revert to disabled state when the dialogue is opened. Users are advised to ensure the toggles represent the entire requested configuration state.

12. Known issues from earlier nShield KeySafe 5 releases

These issues are still present in v1.2.

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.

13. Issues fixed in nShield KeySafe 5 v1.2 OVA Deployment

These fixes are specific to the OVA deployment. Fixes detailed in Issues fixed in nShield KeySafe 5 v1.2 may also be applicable.

Reference	Description

14. Known issues in nShield KeySafe 5 v1.2 OVA Deployment

These issues are specific to the OVA deployment. Issues detailed in Known issues in nShield KeySafe 5 v1.2 and Known issues from earlier nShield KeySafe 5 releases may also be applicable.

Reference	Description
NSE-57638	The host details are lost during an OVA upgrade procedure. Re-enrolling the KeySafe 5 Agent for the host machine will rectify the issue. It is advised that a list of hosts is taken prior to upgrading the OVA.

15. Known issues from earlier nShield KeySafe 5 OVA Deployment releases

These issues are still present in v1.2 of the OVA Deployment. Issues detailed in Known issues from earlier nShield KeySafe 5 releases may also be applicable.

Reference	Description
NSE-53826	KeySafe 5 Appliance Management UI cannot generate an audit log report in XML format. Reports can be generated in CSV format.
NSE-54219	KeySafe 5 Appliance Management UI requires the user to provide a value for the optional 'Name' text field when configuring OIDC for the 'Apply' button to be enabled.
NSE-54314	In a multi-node deployment when switching back to an internal MongoDB database the UI of the other nodes do not show the updated setting, and will not allow further change. From this point onwards any MongoDB settings must be performed on the node which performed the switch back to an internal MongoDB database.
NSE-54377	KeySafe 5 Appliance Management UI does not respond to pressing enter on the keyboard when adding or joining a node to the cluster. Workaround is to use a mouse to the click buttons on the dialogues.
NSE-55024	KeySafe 5 OVA deployment does not allow a nodes hostname to be used as the audience value in the OAUTH2.0 token. This impacts client applications making use of the API, and does not impact the KeySafe 5 UI. Workaround is to use the node IP address as the audience value.
NSE-55099	Unable to restore KeySafe 5 OVA backup to new appliance. When deploying a new appliance and restoring a backup of a previous appliance, the restore will fail. Workaround is to restore to the existing appliance.