KeySafe 5

KeySafe 5 v1.1 Release Notes

21 September 2023

Table of Contents

1. Introduction

These release notes apply to version 1.1 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 v1.1 provides a centralized means to securely manage a distributed nShield HSM estate. This release extends the functionality released in v1.0, specifically in the areas of HSM Feature enablement and Hardserver reporting.

This release provides the option to deploy Keysafe 5 as a virtual appliance (OVA format).

The *Keysafe 5 Installation and Upgrade Guide* and *Keysafe 5 OVA Installation Guide* provides details of how to install, upgrade and use the new platform. Read the appropriate document for the deployment type before installing the platform.

1.2. Versions of these Release Notes

Revision	Date	Description
1.1	2023-05-17	Update to include OVA deployment of Keysafe 5 v1.1
1.0	2022-12-20	Release notes for the release of Keysafe 5 v1.1

2. Features of nShield Keysafe 5 v1.1

The following sections in these release notes detail the specific key features of the 1.1 version of nShield Keysafe 5.

2.1. Host management

Keysafe 5 v1.1 provides the following Host Management operations:

- Listing of Hardserver version
- Listing of Keysafe 5 Agent version
- Ability to group multiple Hosts into a single HSM Pool

2.2. HSM Feature Management

Keysafe 5 v1.1 provides the following HSM Feature Certificate management operations:

- Enable static HSM features
- Enable/Disable dynamic HSM features
- Client Licence upgrades
    - Requires a Keysafe 5 v1.1 agent to be installed on the configured RFS.
- Feature Certificate storage and management
- Perform bulk management of Feature Certificates

2.3. UI Improvements

Keysafe 5 v1.1 provides the following UI improvements:

- Filtering for HSMs, HSM Pools, Hosts and Feature Certificates
- Overall redesign to improve usability
- Performance and responsiveness improvements

2.4. Virtual Appliance

Keysafe 5 v1.1 is provided in OVA format to enable virtual appliance deployments of the Keysafe 5 central platform. This in an alternative to the Kubernetes based

install.

Please see the *Keysafe 5 OVA Installation Guide* for further details.

2.5. Deployment Script

Keysafe 5 v1.1 provides a deployment script to ease the process of installing the Keysafe 5 central platform into a new or existing Kubernetes cluster.

The provisioned environment is intended for evaluation purposes and should *not* be used for production environments without careful consideration. Please see the *Keysafe 5 Installation and Upgrade Guide* for further details.

3. Important information

Before deploying Keysafe 5 v1.1, consider the following points.

3.1. nShield Keysafe 5 agent

nShield Keysafe 5 v1.1 requires that all agents are upgraded to v1.1. 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 contain 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. FIPS SP800-56Ar3

FIPS 140-2 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 introduces new restrictions to the strict-FIPS mode to reflect these new rules.

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.

At present Keysafe 5 v1.1 does not provide the option to enable this compliance

mode when creating or loading the Security World. To enable these restrictions please see the *nShield v12.72 release notes*

Use of this compliance mode has implications on the Remote Administration Cards. See the *nShield v12.72 release notes* for more information. Using this mode is not currently recommended.

3.5. 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. Centralized platform compatibility

4.1. Supported Kubernetes version

This release has been tested on the following Kubernetes versions:

- 1.25

4.2. Supported Istio version

This release has been tested using the following Istio versions:

- 1.15

4.3. Supported external services

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

Software	Minimum Version	Tested Version
MongoDB	4.4	5.0.13
RabbitMQ	3.0	3.11.3

5. 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

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

See the *nShield v12.80 and the v13.3 Security World Software release notes* for further details on supported hardware and platform combinations.

6.3. Supported Security World versions

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

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

Firmware versions supported by the v12.80 and the v13.3 release are also supported by Keysafe 5 v1.1. For additional details on Security World and firmware support, refer to the *nShield v12.80 and the v13.3 Security World software release notes*.

7. Supported identity providers

This release has been tested against the following identity providers:

- Entrust Identity as a Service v5.26
- Microsoft Server 2019 AD FS

Other OIDC and OAuth 2.0 providers might be supported.

8. Keysafe 5 deployment script compatibility

8.1. Supported operating systems

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

- Red Hat Enterprise Linux 8 x64

8.2. 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.

9. Issues fixed in nShield Keysafe 5 v1.1

Reference	Description
NSE-48089	KeySafe 5 Dashboard does not resize correctly
NSE-48117	KeySafe 5 uses deprecated X-XSS-Protection HTTP header
NSE-48231	KeySafe 5 API permits creation of a Softcard without a name
NSE-48436	KeySafe 5 does not apply MongoDB Connection Pool values
NSE-48649	KeySafe 5 cannot pull images stored in an authenticated image registry
NSE-48939	KeySafe 5 fails to install when using TLSv1.3 for RabbitMQ
NSE-51206	KeySafe 5 installs with excessive permissions on the MongoDB secrets mount
NSE-51338	KeySafe 5 Quick start guide deploys MongoDB which cannot be upgraded

10. Known issues in nShield Keysafe 5 v1.1

See also Known issues from earlier nShield Keysafe 5 releases.

Reference	Description
NSE-50294	KeySafe 5 deploy script dry run erroneously reports that it will install istio when it is already installed.
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-51279	During bulk enablement of feature certificates, no option is provided to clear the module(s). The Workaround is to manually clear the module(s) via the HSM details page.
NSE-51644	If an error is reported when enabling a feature in the KeySafe 5 UI, the 'Confirm' button appears to be inactive.
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-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. The workaround is to either increase the 'pollInterval' value, or load the Security World via the Security World information page in the UI.

Reference	Description
NSE-52237	Deletion of a Security World is prevented if a Pool it is loaded on is deleted before deallocating the Pool. The workaround to this is to unload the Security World from a Pool prior to deleting the Pool.
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.

11. Known issues in nShield Keysafe 5 v1.1 OVA Deployment

These issues are specific to the OVA deployment. Issues detailed in Known issues in nShield Keysafe 5 v1.1 and 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.

12. Known issues from earlier nShield Keysafe 5 releases

These issues are still present in v1.1.

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-46050	KeySafe 5 does not support creation of an SP800-56Ar3 compliant Security World. Further information can be found in the Release Notes
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-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