KeySafe 5

KeySafe 5 v1.5.0 Release Notes

13 November 2025

© 2025 Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction

These release notes apply to version 1.5.0 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 nShield Support at nshield.support@entrust.com to request an account.

1.1. Purpose of this release

KeySafe 5 provides a centralized means to securely manage a distributed nShield HSM estate.

This release adds support for managing the nShield 5c 10G HSM, exposes HSM metrics and provides the option to deploy KeySafe 5 as a Windows or Linux Service.

Please see the *Release Package* section of the *KeySafe 5 Installation and Upgrade Guide* for details on the new APIs and services.

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
1.0	2025-10-25	Release notes for KeySafe 5 v1.5.0

2. Features of nShield KeySafe 5 v1.5.0

The following sections in these release notes detail the specific key features of the 1.5.0 version of nShield KeySafe 5.

2.1. nShield 5c 10G support

KeySafe 5 v1.5.0 introduces support for managing the new nShield 5c 10G HSM. For more information on the details of this new nShield HSM, please consult the *nShield 5c 10G release notes*.

This includes support for:

- Network configuration
- Time configuration
- System logging configuration
- Upgrade
- Factory state
- Unit information
- Tenant configuration
- Security World management
- CodeSafe 5 configuration

Please see the *KeySafe 5 User Guide* for more information.

2.2. HSM metrics support

KeySafe 5 v1.5.0 introduces support for exporting HSM metrics in OpenMetrics format. This enables integration with external monitoring systems.

Please see the *KeySafe 5 User Guide* for more information.

2.3. Service Deployment

KeySafe 5 v1.5.0 is now provided in a Windows and Linux Service format to enable installation of KeySafe 5 without the need for a Kubernetes cluster, or an external MongoDB database.

The nShield KeySafe 5 Service Deployment installs alongside the nShield Security World

software.

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

3. Important information

Before deploying KeySafe 5 v1.5.0, consider the following points.

3.1. KeySafe 5 Agent

nShield KeySafe 5 v1.5.0 requires that all KeySafe 5 agents are version v1.3.0 onwards. Running earlier versions of the KeySafe 5 agent will limit certain functionality delivered in this release.

Entrust recommends upgrading all KeySafe 5 agents to v1.5.0 if possible.

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 contain an nShield Edge, you must manually set the HSM mode when you are creating or loading security worlds. Loading worlds on an Edge should be done from the command line. 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

Upgrading from v1.4 to v1.5.0 is supported. Please see the *KeySafe 5 Installation and Upgrade Guide* for more information.

5. Support information

5.1. Kubernetes Deployment

Software	Minimum Version	Tested Version
Kubernetes	1.31	1.33
Istio	1.20	1.21
MongoDB	7.0.14	8.0.13

5.2. Service Deployment

5.2.1. Supported operating systems

The Service Deployment has been tested for compatibility with the following operating sys tems:

- Microsoft Windows Server 2019 x64
- Microsoft Windows Server 2022 x64
- Microsoft Windows Server 2022 Core x64
- Microsoft Windows Server 2025 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

5.2.2. Supported Security World versions

The Service Deployment is compatible with the following nShield Security World software installations:

- Security World v13.6 LTS

5.3. KeySafe 5 Agent compatibility

5.3.1. Supported hardware

The KeySafe 5 Agent supports 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 5c 10G (Base, Mid, High)
- nShield Edge

5.3.2. Supported operating systems

The KeySafe 5 Agent 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 Server 2025 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*.

5.3.3. Supported Security World versions

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

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

Firmware versions supported by the listed releases are also supported by KeySafe 5 v1.5.0. For further details on Security World and firmware support, refer to the *nShield Security World software release notes*.

6. Supported identity providers

This release has been tested against the following identity providers:

- Entrust Identity as a Service v5.44
- Microsoft Server 2019 AD FS

Other OIDC and OAuth 2.0 providers might be supported.

7. Deprecation information

- nShield KeySafe 5 Local is no longer shipped, this has been replaced by the nShield KeySafe 5 Service Deployment.
- RabbitMQ is no longer supported, this has been replaced by a service internal to KeySafe 5. Migration from RabbitMQ is covered in the *KeySafe 5 Installation and Upgrade Guide*.

8. Issues fixed in nShield KeySafe 5 v1.5.0

Reference	Description
NSE-66868	updateinternalcerts.sh unable to restart MongoDB after certs expired
NSE-69438	No Event ID is repeatedly reported in Event Viewer

9. Known issues in nShield KeySafe 5 v1.5.0

See also Known issues from earlier nShield KeySafe 5 releases.

Reference	Description
NSE-69741	When many (tens of thousands of) files are added to the kmdata/local directory at once, a 'queue or buffer overflow' error may appear in KeySafe 5 agent logs. Restart the KeySafe 5 agent and if the problem persists, remove these files fromm kmdata/local and introduce files to the kmdata/local directory in smaller batches.
NSE-69761	Occasionally Security World operations may fail part way through the authorisation process, if this happens please try again.
NSE-70502	Upgrading firmware on multiple HSMs at the same time can occasionally cause an 'error storing upgrade image'. If this occurs please try again once other firmware upgrades have finished.
NSE-71678	The loading of security worlds onto a large number of HSMs can time out. If this happens, either go back to the previous page and try again or reduce the number of HSMs for each load request.
NSE-72656	When trying to save an Agent configuration file, selecting certain cipher suites from the drop down list will result in an invalid agent. This is currently not configurable.
NSE-73268	A 500 error can occur when downloading the Agent logs, if this happens please try again.
NSE-73274	A 500 error can occur when downloading the System logs, if this happens please try again.
NSE-73318	Duplicate slots can be added to a HSM's 'Slot Export' section.
NSE-73951	KeySafe 5 installers show as a random filename during the User Account Control pop-up, such as '61e12.msi'.

10. Known issues from earlier nShield KeySafe 5 releases

These issues are still present in v1.5.0.

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.
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.

Reference	Description
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-64712	As the number of secrets grows in the KeySafe 5 database, operations such as obtaining counts and distinct values can start to fail depending on the CPU & memory resource available to the database server and timeout value set on the connection. If this occurs the recommendation is to increase the resources available to the database server and increase the database.mongo.socketTimeout value in the backend helm chart.
NSE-65357	When the user is configuring KCM on the KeySafe5 UI, on the token or key selection page, starting on the default 5 items per page and clicking the next button and changing the items per page to a different number causes number of key doesn't not match to the same items per page. This can be reset by going back to the first page and setting you items back to default.