KeySafe 5

KeySafe 5 v1.6.1 Release Notes

30 September 2025

Table of Contents

1. Introduction

These release notes apply to version 1.6.1 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 provides a centralized means to securely manage a distributed nShield HSM estate. The v1.6.1 release delivers new functionality to monitor nShield HSM estate operations by allowing access to live and historical metrics as well as the ability to create customizable system alerts. These new features are enabled through the purchase of a license. Please contact your Entrust account manager for licensing and pricing information.

KeySafe 5 v1.6.1 is intended to replace the functionality previously provided by the discontinued product, nShield Monitor.

Please see the *Release Package* section of the *KeySafe 5 Installation and Upgrade Guide* for details on the new APIs, helm charts 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	2025-09-30	Release notes for KeySafe 5 v1.6.1 GA

2. Features of nShield KeySafe 5 v1.6.1

The following sections in these release notes detail the specific key features of the 1.6.1 ver sion of nShield KeySafe 5.

2.1. Monitoring and Alerting of nShield HSM estates

KeySafe 5 v1.6.1 provides new capabilities of monitoring HSMs enrolled to KeySafe 5. This feature provides real time metrics collection to be able to create custom alerting triggers for Security World environments with HSMs installed or enrolled, such as fan failure, max temperature levels, capacity throughput, memory usage, client licenses, and HSM/host states. Also provides historical graphs of the collected metric data.

KeySafe 5 v1.6.1 Estate Monitoring provides Open metrics format when accessing KeySafe 5 v1.6.1 rest API. Custom Alerting notifications can be sent out using email and using Web-hooks.

KeySafe 5 v1.6.1 is the new way to monitor your HSM estate. It supports several features that were part of nShield Monitor, which has reached end-of-life.

3. Important information

Before deploying KeySafe 5 v1.6.1, consider the following points.

3.1. KeySafe 5 v1.6.1 Estate Monitoring License

To enable the new feature of Estate Monitoring a license needs to be applied. To be able to request a license, a unique identifier is required to associate the license with the installation instance. This unique identifier is created during system installation. For details on where to find it, see the *Licence management* section of the *Estate management using the KeySafe 5 WebUI* page in the *KeySafe 5 User Guide*. For further information about licenses and pricing information, please contact Entrust nShield Technical Support at nshield.support@entrust.com.

3.2. nShield KeySafe 5 Agent

nShield KeySafe 5 v1.6.1 requires that all agents are upgraded to v1.6.1. Differing versions between the central platform and agent is not supported.

3.3. 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 behavior of the kmdata synchronization will be impacted. KeySafe 5 Host Management will highlight issues of clock skew in the health of a Host resource.

3.4. 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.

3.5. 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.

3.6. Included MongoDB Helm Charts and Images

There has been an update to the deployment scripts of third party dependencies for Kubernetes installations. These now allow the use of locally shipped containers. The ability to use existing MongoDB instances is unchanged.

4. Upgrade information

Upgrading from v1.4 to v1.6.1 is supported. Please see the *Upgrade* section of the *KeySafe 5 Installation and Upgrade Guide* for more information.

5. Centralized platform compatibility

5.1. Supported Kubernetes version

Software	Minimum Version	Tested Version
Kubernetes	1.31	1.33

5.2. Supported Istio version

Software	Minimum Version	Tested Version
Istio	1.20	1.21

5.3. Supported external services

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

Software	Minimum Version	Tested Version
MongoDB	7.0.14	8.0.13

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 Server 2025
- 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 v13.6 LTS

Firmware versions supported by the listed releases are also supported by KeySafe 5 v1.6.1. For further details on Security World and firmware support, refer to the *nShield Security World software release notes*.

7. Supported identity providers

This release has been tested against the following identity providers:

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

Other OIDC and OAuth 2.0 providers might be supported.

8. Deprecation information

RabbitMQ is no longer supported with nShield KeySafe 5 v1.6.1.

9. Issues fixed in nShield KeySafe 5 v1.6.1

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.
NSE-64436	The KeySafe 5 UI can not browse directly to a certificate using the URL.

10. Known issues in nShield KeySafe 5 v1.6.1

See also Known issues from earlier nShield KeySafe 5 releases.

Reference	Description
NSE-72709	When adding Webhook alert methods to a Trigger via the search, an error may happen when trying to find a match if an existing Webhook is pasted in completely. Instead the value should be entered in manually and then the appropriate suggestion can be selected.
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-72609	If a large clock skew event occurs and is corrected, UI visualizations can fail to render. They should reappear once the system has progressed farther than the incorrectly skewed time value.
NSE-72525	The Object Count Alert Type uses the difference between two different OpenMetrics counters. The counters can independently wrap around when they overflow and if this happens, it can fire a false positive alert. When both counters have wrapped around, the difference calculation will be as expected and the false positive alert will be resolved.
NSE-72181	The Transactions graph for HSMs and Hosts can display an anomalous spike. This can be caused by irregular data, perhaps from a resource reset. The graph will return to expected values when the irregular data is outside the scope of the request, either by refreshing the graph or changing the time interval.
NSE-71687	The nShield Edge is not supported in KeySafe 5 for World loading or Upgrade management.
NSE-71678	The loading of security worlds onto a large number of multiple 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-71588	Notifications for resolved Alerts can get missed if a Trigger is edited at precisely the wrong time. This only affects the notifications of resolved and there are no issues with the firing of new Alerts.
NSE-70413	When using 32 bit Firefox in alert configuration and Alert Type is selected all static text is highlighted as mouse is moved over the page. This does not effect the functionality of the page.
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.

11. Known issues from earlier nShield KeySafe 5 releases

These issues are still present in v1.6.1.

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-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.

12. Post-release documentation changes and corrections for the v1.6.1 release

The following documentation changes have been made since v1.6.1 was released:

No change since release.