KeySafe 5

KeySafe 5 v1.7.0 Release Notes

8 April 2026

Table of Contents

1. Introduction

These release notes apply to version 1.7.0 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 Monitoring and Alerting using KeySafe 5 as a Windows or Linux Service, combining support for all nShield hardware platforms.

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	2026-04-08	First set for KeySafe 5 v1.7

2. Features of nShield KeySafe 5 v1.7.0

The following sections in these release notes detail the specific key features of the 1.7.0 version of nShield KeySafe 5.

2.1. Service Deployment

KeySafe 5 v1.7.0 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.

The service deployment combines the two previous releases and supports both the nShield 5c 10G support and v1.6 release of Monitoring and Alerting as part of the Service Deployment.

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

2.2. MongoDB support in Service Deployment

KeySafe 5 v1.7.0 now provides, as part of the Service Deployment, the ability to use either MongoDB as your chosen database or SQLite as the default database.

2.3. Support FIPS 186-5 compliant security worlds

KeySafe 5 v1.7.0 now supports the creation of the new Security World cipher suite ECp521-mAES and corresponding KML type NISTp256hSHA1.

The new cipher suite is only available from 13.9.3 security world supported software and corresponding 13.8.4 firmware. To load an ECp521-mAES Security World on a module, HSMs must be running this version.

2.4. Update to SP800-56Ar3 Security World Flag

KeySafe 5 v1.7.0: As of version 13.9.3 security world software, the SP800-56Ar3 flag is set by default when creating a FIPS-140-level3 security world. It cannot be selected manually at world creation time.

2.5. Unlicensed Metrics data visibility increased to 7 days

KeySafe 5 v1.7.0 makes available historical metrics data for a rolling seven days. For longer-term historical data, a Monitoring and Alerting license is required.

2.6. Updates to CSP Secrets Management Integration

KeySafe 5 v1.7.0 has updated how you can connect to the CSP compliance manager by selecting or dropping the KCM JSON file to configure the connection, as opposed to having to do this by hand.

3. Important information

Before deploying KeySafe 5 v1.7.0, consider the following points.

3.1. KeySafe 5 Agent

nShield KeySafe 5 v1.7.0 requires that all KeySafe 5 agents are version v1.3.0 or later. Running earlier versions of the KeySafe 5 agent will limit certain functionality delivered in this release.

Entrust recommends upgrading all KeySafe 5 agents to v1.7.0 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 v1.5 or v1.6 to v1.7.0 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	1.33	1.35
Istio	1.28	1.28
MongoDB	7.0.x	8.0.x

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 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
- Red Hat Enterprise Linux 10 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 8 x64
- Oracle Enterprise Linux 9 x64
- Amazon Linux 2023 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 (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 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
- Red Hat Enterprise Linux 10 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 8 x64
- Oracle Enterprise Linux 9 x64
- Amazon Linux 2023 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
- Security World v13.9 STS

Firmware versions supported by the listed releases are also supported by KeySafe 5 v1.7.0. 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 2022 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 v1.7.0

Reference	Description
NSE-70413	When using 32-bit Firefox in alert configuration and Alert Type is selected, static text is no longer highlighted as the mouse is moved over the page.
NSE-72656	When selecting cipher suites from the drop down list in the Agent configuration page no longer results in an invalid agent.
NSE-73506	Prometheus and alert manager can now be deployed using local registries as well as external registries
NSE-73951	KeySafe 5 Windows installers no longer show as a random filename during the User Account Control pop-up; this now shows the standard MSI installer name
NSE-74101	KeySafe 5 Agent install on Linux now creates the required folder structure and files for you, providing the necessary certificate request to get the Agent certificate setup.

9. Known issues in nShield KeySafe 5 v1.7.0

See also Known issues from earlier nShield KeySafe 5 releases.

Reference	Description
NSE-73087	When managing Tenant system logs on 5c 10g you are unable to use a separate network pro file.
NSE-75788	When generating a FIPS-140-level3 security world through KeySafe 5 and then loading this world on a 13.6.x client the Security World will not be usable. To overcome this issue, edit the world to disable StrictKeyAgreement SP800-56Ar3 flag. In the KeySafe 5 UI. 1. World → Actions → Update World 2. Toggle "Require the enabling of SP800-56Ar3 restrictions" to disabled in the world set- tings in the world file 3. Authorize the operation by presenting the admin card. At this point, the world will start working on the 13.6.x host side as the world kmdata file has been updated on the host. A second step is required to re-load the security world enabling SP800-56Ar3 restrictions. This will re-enable SP800-56Ar3 at world loading time to be fully FIPS-140-level3 compliant in a 13.6.x client setup. 4. Unauthorize the Security World from the pool so that it can be re-loaded. 5. Authorize the world into the pool and make sure to toggle "SP800-56Ar3 Compliance" to ON for the modules being loaded in the world. For further information, please contact Entrust support. See also https://nshielddocs.entrust.com/security-world-docs/secworld-admin/security-worlds.html#_nist_sp800_56ar3
NSE-76520	There is an issue where module fan metrics are not available for Solo+ devices. This also means that fan speed visuals are not available in the UI for Solo+ devices.
NSE-76521	There is an issue where module temperature metrics are not available for Solo+ devices. This also means that current temperature percentage visuals are not available in the UI for Solo+ devices.
NSE-76177	When configuring the 5c 10g through Keysafe 5, it is not possible to use TCP ports with sys log. Use UDP for syslog output instead.
NSE-77444	When allocating a Security World to another pool, clicking CONFIRM executes the opera- tion but does not update the page beyond displaying "Operation successful" at the top. Nav igate to another top menu item, then return to confirm that the Security World is now in the new pool.
NSE-77082	Revealing metadata on EC and KCDSA keys requires the corresponding feature to be enabled on all HSMs in the Pool.

Reference	Description
NSE-77215	When reporting HSM information on SoloXC and 5s, remaining client licenses are shown. Solo XC and 5s do not have client licenses so this should be ignored.
NSE-77334	The Agent can stop sending kmdata updates after a recent Security World deallocation operation. This issue occurs occasionally and can be resolved by restarting the Agent.

10. Known issues from earlier nShield KeySafe 5 releases

These issues are still present in v1.7.0.

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-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 from kmdata/local and introduce files to the kmdata/local directory in smaller batches.
NSE-69761	Occasionally Security World operations may fail partway through the authorization 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-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 an HSM's 'Slot Export' section.