



ENTRUST

KeySafe 5

KeySafe 5 v1.4 Release Notes

16 October 2024

Table of Contents

1. Introduction	1
1.1. Purpose of this release	1
1.2. Versions of these Release Notes	1
2. Features of nShield KeySafe 5 v1.4	2
2.1. Entrust KeyControl Compliance Manager	2
3. Important information	3
3.1. nShield KeySafe 5 agent	3
3.2. Key Management Data Synchronization	3
3.3. nShield Edge	3
3.4. Remote Administration Authorized Card List	3
4. Upgrade information	4
5. Centralized platform compatibility	5
5.1. Supported Kubernetes version	5
5.2. Supported Istio version	5
5.3. Supported external services	5
6. KeySafe 5 agent compatibility	6
6.1. Supported hardware	6
6.2. Supported operating systems	6
6.3. Supported Security World versions	7
7. KeySafe 5 Local compatibility	8
7.1. Supported hardware	8
7.2. Supported operating systems	8
7.3. Supported Security World versions	8
8. Supported identity providers	10
9. KeySafe 5 deployment script compatibility	11
9.1. Supported operating systems	11
9.2. Supported versions of software	11
10. Deprecation information	12
11. Issues fixed in nShield KeySafe 5 v1.4	13
12. Known issues in nShield KeySafe 5 v1.4	14
13. Known issues from earlier nShield KeySafe 5 releases	15
14. Post-release documentation changes and corrections for the v1.4 release	17

1. Introduction

These release notes apply to version 1.4 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 v1.4 provides a centralized means to securely manage a distributed nShield HSM estate. This release extends the functionality released in v1.3, adding key compliance management functionality.

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	2024-08-27	Release notes for KeySafe 5 v1.4
1.1	2024-10-16	Added new Release Note section for post-release documentation changes: Post-release documentation changes and corrections for the v1.4 release.

2. Features of nShield KeySafe 5 v1.4

The following sections in these release notes detail the specific key features of the 1.4 version of nShield KeySafe 5.

2.1. Entrust KeyControl Compliance Manager

KeySafe 5 v1.4 provides functionality to connect to Entrust KeyControl Compliance Manager. This integration provides the means of running compliance profiles across an estate of Security World keys and allows keys to be documented.

The following operations are now possible:

- Creating a connection to the Entrust KeyControl Compliance Manager for a specific Security World.
- Synchronization of key metadata to the Entrust KeyControl Compliance Manager instance.
- Updating connection settings.
- Revoking the connection to the Entrust KeyControl Compliance Manager.

To connect to an instance of Entrust KeyControl Compliance Manager firstly obtain an AppLink token and ID from the Entrust KeyControl Compliance Manager instance, then from KeySafe 5 initiate the connection wizard via the "Compliance Manager" tab under the Security World details view.

Contact Entrust nShield Technical Support at nshield.support@entrust.com to request more information regarding Entrust KeyControl Compliance Manager.

3. Important information

Before deploying KeySafe 5 v1.4, consider the following points.

3.1. nShield KeySafe 5 agent

nShield KeySafe 5 v1.4 requires that all agents are upgraded to v1.4. 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.

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 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.

4. Upgrade information

Upgrading from KeySafe 5 v1.3 to KeySafe 5 v1.4 is supported.

The *KeySafe 5 Installation and Upgrade Guide* provides details of how to upgrade the platform.

5. Centralized platform compatibility

5.1. Supported Kubernetes version

This release has been tested on the following Kubernetes versions:

- 1.29

5.2. Supported Istio version

This release has been tested using the following Istio versions:

- 1.22

5.3. Supported external services

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

Software	Minimum Version	Tested Version
MongoDB	6.0	6.0.16
	7.0	7.0.11
RabbitMQ	3.0	3.13.3

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
- 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 v13.4
- Security World v13.6

Firmware versions supported by the listed releases are also supported by KeySafe 5 v1.4. For further details on Security World and firmware support, refer to the *nShield Security World software release notes*.

7. KeySafe 5 Local 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 2019 x64
- Microsoft Windows Server 2022 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

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 v13.6

Firmware versions supported by the listed releases are also supported by KeySafe 5 v1.4. 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 v5.33
- Microsoft Server 2019 AD FS



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



Vertical line | Versions of OpenSSL below 1.1.1 are not supported.

10. Deprecation information

In an upcoming release of nShield KeySafe 5 RabbitMQ support will be removed.

11. Issues fixed in nShield KeySafe 5 v1.4

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.

12. Known issues in nShield KeySafe 5 v1.4

See also [Known issues from earlier nShield KeySafe 5 releases](#).

Reference	Description
NSE-64712	<p>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.</p> <p>If this occurs the recommendation is to increase the resources available to the database server and increase the <code>database.mongo.socketTimeout</code> value in the backend helm chart.</p>
NSE-64998	<p>On certain platforms KeySafe 5 Local is unable to upload a file from a mounted directory such as an ISO.</p> <p>The workaround is to copy the file to a local directory prior to uploading.</p>

13. Known issues from earlier nShield KeySafe 5 releases

These issues are still present in v1.4.

Reference	Description
NSE-37786	<p>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.</p> <p>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.</p>
NSE-46785	<p>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.</p> <p>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.</p> <p>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.</p>
NSE-51100	<p>KeySafe 5 does not enforce the Remote Administration authorized card list.</p> <p>Further information can be found in the Release Notes</p>
NSE-51114	<p>When running the deploy.sh script with DOCKER_REGISTRY set, Docker images can not be pulled from an authenticated Docker registry.</p> <p>The workaround is to not set DOCKER_REGISTRY and the deploy script will spin up its own registry for use.</p>
NSE-52265	<p>KeySafe 5 can not disable SEE Activation (Restricted) unless all hosts in the HSM Pool are healthy at the time of the disable action.</p> <p>The workaround is to manually remove the feature enablement certificate files from the host machine.</p>
NSE-56419	<p>KeySafe 5 allows the creation of an SP800-56Ar3 Security World using v1.0 Java cards.</p> <p>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.</p>
NSE-56722	<p>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.</p>

Reference	Description
NSE-57196	<p>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.</p> <p>The workaround is to ensure that the nShield 5c kmdata is deleted prior to removing from KeySafe 5.</p>

14. Post-release documentation changes and corrections for the v1.4 release

The following documentation changes have been made since v1.4 was released:

Reference	Date	Description
NSE-66508	2024/10/16	Minor filepath and command fixes in the Install on Linux section of the Quick-start Guide.