KeySafe 5

KeySafe 5 v1.0 Release Notes

8 April 2024

Table of Contents

1. Introduction

These release notes apply to version 1.0 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 Entrust nShield Technical Support at nshield.support@entrust.com to request an account.

1.1. Purpose of this release

KeySafe 5 1.0 provides a centralized means to securely manage a distributed nShield HSM estate. This includes managing and creating Security Worlds and associated resources (Softcards and Card Sets).

The *KeySafe 5 Installation Guide* provides details of how to install and use the new platform. Read this document before installing the platform.

If the v0.90 preview release of the KeySafe 5 was used as part of preview release testing; that version should be un-installed and this v1.0 release installed. See the *KeySafe 5 Installation Guide* for details on how to uninstall the preview.

1.2. Versions of these Release Notes

Revision	Date	Description
1.0	2022-5-12	Release notes for the first release of KeySafe 5 v1.0

2. Concepts of nShield KeySafe 5

2.1. nShield KeySafe 5

KeySafe 5 is a system to allow the management of an estate of HSMs through an intuitive web-based UI. The system also contains a RESTful API which can be used directly if required to provide custom management of the estate.

KeySafe 5 consists of a web API back end that uses MongoDB, a web UI front end, and the API gateway Istio, that handles authentication.

The main central management platform of KeySafe 5 is deployed as a Kubernetes application. For each nShield client machine that you want to manage using this platform, you must install a KeySafe 5 agent alongside the existing nShield hardserver.

2.2. nShield KeySafe 5 agent

The KeySafe 5 agent is installed on computers attached to HSMs and running the hardserver. The KeySafe 5 agent ensures that all key management data, with the exception of keys, is synchronised between the nShield client machine and the central (MongoDB) database. Communications between the agent and the back end are handled through the RabbitMQ message broker.

2.3. HSM Pool

An HSM Pool is a collection of HSMs that are managed together. For example, loading a Security World on an HSM Pool will result in that Security World being loaded onto all the HSMs in the pool. In the current version an HSM Pool will be the collection of HSMs communicating with a single hardserver and a single KeySafe 5 agent.

The KeySafe 5 agent synchronises the state of the HSM Pool with the back end, and performs actions on its behalf. If you create a new card set or softcard, either through KeySafe 5 or manually, it will be synchronised to all the HSM Pools in the same Security World. If you make a deletion through KeySafe 5, such as deleting a softcard, that deletion will be applied by the agent to all KeySafe 5 HSM Pools in the same Security World. However if you delete a softcard without going through KeySafe 5, that deletion will not be applied to other HSM Pools in the same

Security World.

2.4. HSM

Unless network-connected, an HSM can only be in one pool at any one time, but may be moved between machines in the usual manner, and KeySafe 5 will reflect this change. An HSM may have the HSM Pool's Security World loaded.

An nShield Connect may be enrolled into multiple HSM Pools, but it can only have one active Security World at a time.

2.5. Security World

A Security World may be loaded on multiple HSM Pools.

2.6. Operations and authorizations

When performing an operation on the command-line, like creating a Security World, specifying all the parameters, and then inserting all the cards and typing their passphrases has to be done in one step. With KeySafe 5 this is separated into two steps: creating an operation, and then authorising it. When creating an operation all the parameters for that operation are requested, and then it is listed in the *Outstanding Operations* list against the Security World to which it belongs.

Whenever a user is required to present a card or a passphrase to complete an operation, an authorization is created. For example:

- Security World creation requires writing a new Administrator Card Set so will require 'BlankCard' authorizations.
- Security World loading requires presenting an existing Administrator Card Set so will require 'AdminCard' authorizations.
- Operator Card Set creation requires writing a new Operator Card Set so will require 'BlankCard' authorizations.
- Softcard creation requires setting a passphrase so will require a 'Passphrase' authorization.

If there is a specific order that the authorizations must be provided then a subset of the authorizations may initially be in 'Blocked' state.

Example One:

In a FIPS-140-2-level-3 Security World, operations such as OCS or softcard creation require an initial FIPS authorization (presentation of an Administrator or Operator card from the Security World) to authorize the operation. In this case a 'FIPS' authorization is created that must be completed before any other authorization types.

Example Two:

Creating a Security World with a quorum of 2/4 cards in the ACS on a pool with 2 HSMs results in 6 authorization requests. The first 4 will be to create the Administrator Card Set on one HSM, and the subsequent 2 will be to load the Security World onto the other HSM.

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. Features of nShield KeySafe 5 v1.0

The following sections in these release notes detail the specific key features of the 1.0 version of nShield KeySafe 5.

3.1. HSM management

KeySafe 5 v1.0 provides the following HSM Management operations:

- HSM information (enquiry)
- HSM mode change
- HSM clear
- HSM Slot information
- HSM Slot formatting

3.2. Security World management

KeySafe 5 v1.0 provides the following Security World management operations:

- Security World information and kmdata download
- Security World creation
- Security World loading
- Security World removal (erase module)
- Replace ACS
- ACS card passphrase change
- Card Set information and kmdata download
- Card Set creation
- Card Set passphrase change
- Card Set passphrase recovery
- Card Set removal
- Softcard information and kmdata download
- Softcard creation
- Softcard passphrase change
- Softcard passphrase recovery
- Softcard removal

4. Important information

Before deploying KeySafe 5 v1.0, consider the following points:

- KeySafe 5 takes ownership over certain kmdata synchronization (world, module certs, Card Sets and Softcards), and as such might conflict with existing methods.
- 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 in nShield KeySafe 5 v1.0.

5. Centralized platform compatibility

5.1. Supported Kubernetes version

This release has been tested on the following Kubernetes versions:

- 1.22

5.2. Supported Istio version

This release has been tested using the following Istio versions:

- 1.13

5.3. Supported external services

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

Software	Minimum Version	Tested Version
MongoDB	4.0	4.4.12
RabbitMQ	3.0	3.9.13

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 2019 x64
- Microsoft Windows Server 2019 Core x64
- Microsoft Windows Server 2016 x64
- Microsoft Windows Server 2012 R2 x64
- Microsoft Windows 10 x64
- Red Hat Enterprise Linux AS/ES 6 x64
- Red Hat Enterprise Linux AS/ES 7 x64
- Red Hat Enterprise Linux AS/ES 8 x64
- SUSE Enterprise Linux 12 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 6 x64
- Oracle Enterprise Linux 7 x64
- Oracle Enterprise Linux 8 x64

See the *nShield 12.80 and 13.2 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 v13.2

Firmware versions supported by the 12.80 and 13.2 release are also supported by KeySafe 5 v1.0. For additional details on Security World and firmware support, refer to the *nShield 12.80 and 13.2 Security World software release notes*.

7. Supported identity providers

This release has been tested against the following identity providers:

- Entrust Identity as a Service v5.16
- Microsoft Server 2019 AD FS

Other OIDC and OAuth 2.0 providers might be supported.

8. Known issues in nShield KeySafe 5 v1.0

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-46050	KeySafe 5 does not support creation of an SP800-56Ar3 compliant Security World
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.