KeySafe 5

# KeySafe 5 v1.8.0 Release Notes

20 November 2026

© Entrust Corporation. All rights reserved.

# 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 v1.8.0 . . . 2
    2.1. nShield 5c 10G Initial Configuration Service (NSE-77073) . . . 2
    2.2. Additional metrics for nShield 5c 10G (NSE-77073) . . . 2
    2.3. Support for Bootloader upgrade and Recovery images (NSE-64926) . . . 2
    2.4. FPGA cryptographic acceleration selection (NSE-76606) . . . 2
    2.5. Support for Microsoft Entra ID (NSE-79325) . . . 2
    2.6. Support for static routes on 5c 10G (NSE-77057) . . . 3
    2.7. Multilevel PKI certificate support (NSE-76850) . . . 3
    2.8. Alerts for CodeSafe 5 certificate expiration (NSE-76875) . . . 3
3. Important information . . . 4
    3.1. KeySafe 5 Agent . . . 4
    3.2. Key Management Data Synchronization . . . 4
    3.3. nShield Edge . . . 4
    3.4. Remote Administration Authorized Card List . . . 4
4. Upgrade information . . . 5
5. Support information . . . 6
    5.1. Kubernetes Deployment . . . 6
    5.2. Service Deployment . . . 6
        5.2.1. Supported operating systems . . . 6
        5.2.2. Supported Security World versions . . . 6
    5.3. KeySafe 5 Agent compatibility . . . 7
        5.3.1. Supported hardware . . . 7
        5.3.2. Supported operating systems . . . 7
        5.3.3. Supported Security World versions . . . 7
6. Supported identity providers . . . 9
7. Deprecation information . . . 10
8. Issues fixed in nShield KeySafe 5 v1.8.0 . . . 11
9. Known issues in nShield KeySafe 5 v1.8.0 . . . 12
10. Known issues from earlier nShield KeySafe 5 releases . . . 13

# 1. Introduction

These release notes apply to version 1.8.0 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 updates for managing the nShield 5c 10G HSM, and exposes additional HSM metrics.

For details about the new APIs and services, see the Release Package section of the KeySafe 5 Installation and Upgrade Guide.

The KeySafe 5 Installation and Upgrade Guide explains 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 | 2026-11-10 | Release notes for KeySafe 5 v1.8.0 |

# 2. Features of nShield KeySafe 5 v1.8.0

The following sections in these release notes detail the specific key features of the 1.8.0 ver sion of nShield KeySafe 5.



Unless otherwise specified, the features described in these release notes apply to all supported deployments of nShield KeySafe 5.

For more information, see the KeySafe 5 User Guide.

## 2.1. nShield 5c 10G Initial Configuration Service (NSE-77073)

KeySafe 5 v1.8.0, when used with nShield 5c 10G HSM image version v14.4.2 or later, requires only the IP address of your nShield 5c 10G HSM to fully enroll the HSM. You can obtain the IP address directly from the HSM. For more information about obtaining the IP address, see the *nShield 5c 10G Quick Start Guide*.

## 2.2. Additional metrics for nShield 5c 10G (NSE-77073)

KeySafe 5 v1.8.0 introduces support for disk wear (NVMe storage) and uptime metrics for the nShield 5c 10G HSM. Disk wear health status can be configured as a custom alert.

## 2.3. Support for Bootloader upgrade and Recovery images (NSE-64926)

KeySafe 5 v1.8.0 introduces support for upgrading the bootloader and recovery images on the nShield 5s and 5c 10G HSMs.

## 2.4. FPGA cryptographic acceleration selection (NSE-76606)

A user can now select the desired FPGA cryptographic acceleration image for the nShield 5s or 5c 10G HSM. Select the hybrid (HY) cryptographic accelerator, which is optimized for post-quantum cryptography, or the default (PK) cryptographic accelerator.

## 2.5. Support for Microsoft Entra ID (NSE-79325)

KeySafe 5 v1.8.0 now supports integration with Microsoft Entra ID as an identity provider (IDP) for authentication and authorization.

## 2.6. Support for static routes on 5c 10G (NSE-77057)

KeySafe 5 v1.8.0 now supports the configuration of static routes for the nShield 5c 10G HSM using the UI or the API.

## 2.7. Multilevel PKI certificate support (NSE-76850)

KeySafe 5 v1.8.0 introduces support for multilevel PKI certificates.

## 2.8. Alerts for CodeSafe 5 certificate expiration (NSE-76875)

KeySafe 5 v1.8.0 now provides default alerts for CodeSafe 5 certificate expiration. These alerts are available out of the box and do not require a Monitoring or Estate Monitoring license.

# 3. Important information

Before deploying KeySafe 5 v1.8.0, consider the following points.

## 3.1. KeySafe 5 Agent

nShield KeySafe 5 v1.8.0 requires that all KeySafe 5 agents are version v1.5.0 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 v1.8.0 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 v1.7 to v1.8.0 is supported. For more information, see the KeySafe 5 Installation and Upgrade Guide.

# 5. Support information

## 5.1. Kubernetes Deployment

| Software | Minimum Version | Tested Version |
|---|---|---|
| Kubernetes | 1.34 | 1.36 |
| Istio | 1.30 | 1.30 |
| 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 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

### 5.2.2. Supported Security World versions

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

- Security World v13.6.x LTS
- Security World v13.9.x STS

## 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 Connect XC (Base, Mid, High, Serial Console)
- 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 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

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 v13.6x LTS
- Security World v13.9x STS

Firmware versions supported by the listed releases are also supported by KeySafe 5 v1.8.0. 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 v5.46
- Microsoft Entra ID
- Microsoft Server 2019 AD FS



Other OIDC and OAuth 2.0 providers may work but are not officially sup ported.

# 7. Deprecation information

- nShield KeySafe 5 Local is no longer shipped, this has been replaced by the nShield KeySafe 5 Service Deployment.

# 8. Issues fixed in nShield KeySafe 5 v1.8.0

| Reference | Description |
|---|---|
| NSE-69050 | When deploying a Codesafe 5 image when another one is currently running or stopped. |
| NSE-72656 | When trying to save an Agent configuration file, selecting certain cipher suites from the drop-down list resulted in an invalid Agent. The cipher suites are now configurable. |
| NSE-72709 | When pasting webhooks that contain special characters, errors are displayed. |
| NSE-73951 | When installing KeySafe 5, the installer appeared as a random filename, such as 61e12.msi, in the User Account Control pop-up. This issue has been fixed, and the correct installer file-name is now displayed. |
| NSE-76177 | When configuring the 5c 10G through KeySafe 5, TCP ports cannot be used with syslog. Use UDP for syslog output instead. |
| NSE-77082 | When revealing metadata on EC keys, the Elliptic Curve feature must be enabled on the cor responding host machine. |
| NSE-79951 | Invalid content in the alert manager config file prevents startup. For example, an empty smart host port number. |
| NSE-80169 | Setting the sp80056ar3 flag on an unrestricted world in KeySafe 5 causes the world to become unusable. |

# 9. Known issues in nShield KeySafe 5 v1.8.0

See also Known issues from earlier nShield KeySafe 5 releases.

| Reference | Description |
|---|---|
| NSE-56419 | KeySafe 5 allows the creation of an SP800-56Ar3 Security World using v1.0 Java cards.<br><br>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-80195 | You are unable to upload the SSHD CodeSafe 5 client key through the KeySafe 5 UI. To work around this issue, use the API endpoint.<br><br>curl -k -X PUT <your IP>/codesafe/v1/machines/<machineid>/sshdclientkey -H 'Content-Type: application/json' -d '{"keytype": "ecdsa-sha2-nistp256"\, "keydata": "ZWNkc2E..... NpcGhlci5jb20K"}' |
| NSE-79881 | CodeSafe 5 logging is always enabled even when explicitly disabled. |
| NSE-80764 | After a factory reset of an nShield 5c 10G, the HSM may reappear in KeySafe 5 and be reported as unhealthy. Remove the corresponding HSM record to resolve the issue. |

# 10. Known issues from earlier nShield KeySafe 5 releases

These issues are still present in v1.8.0.

| 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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>The workaround is to manually remove the feature enablement certificate files from the host machine. |
| 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. |
| 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.<br><br>The workaround is to ensure that the nShield 5c kmdata is deleted prior to removing from KeySafe 5. |

| Reference | Description |
|---|---|
| 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.<br><br>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 CSP/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. |
| NSE-69741 | When many files (tens of thousands) are added to the kmdata/local directory at once, a 'queue or buffer overflow' error may appear in the KeySafe 5 agent logs. Restart the KeySafe 5 agent. If the problem persists, remove the files from kmdata/local and add them back to the directory in smaller batches. |
| NSE-69761 | Security World operations may occasionally fail partway through the authorization process. If this happens, try again. |
| NSE-70502 | Upgrading firmware on multiple HSMs at the same time can occasionally cause an 'error storing upgrade image'. If this occurs, try again after the other firmware upgrades have finished. |
| NSE-71678 | Loading security worlds onto a large number of HSMs can time out. If this happens, return to the previous page and try again, or reduce the number of HSMs in each load request. |
| NSE-73268 | A 500 error can occur when downloading the Agent logs. If this happens, try again. |
| NSE-73274 | A 500 error can occur when downloading the System logs. If this happens, try again. |