KeySafe 5

KeySafe 5 v1.6.1 User Guide

17 October 2025

Table of Contents

1. Introduction

The KeySafe 5 platform (KeySafe 5) is a system to enable the management of an estate of HSMs through a web-based graphical user interface. KeySafe 5 also contains a REST API which can be used directly if required to provide custom management of the estate.

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

For additional information on installing, upgrading, and deploying KeySafe 5, refer to the Installation and Upgrade guide.

1.1. KeySafe 5 architecture

1.1.1. Host Machines

Each host machine can have one or more HSMs installed, and a single Security World. The HSM estate monitored by KeySafe 5 is located on one or more host machines.

For each nShield host machine that you want to manage with KeySafe 5, you must install a KeySafe 5 agent alongside the existing nShield hardserver on the host machine, see nShield KeySafe 5 agent.

1.1.2. nShield KeySafe 5 agent

On each host machine in your estate that you want to monitor with KeySafe 5, the KeySafe 5 agent service is required. The KeySafe 5 agent runs alongside the existing hardserver. The KeySafe 5 agent ensures that all key management data, with the exception of keys, is synchronised between the nShield host machine and the central database. This information is then shared with each host machine in the Security World that has the KeySafe 5 agent running.

1.1.3. HSM Pool

An HSM Pool is a collection of HSMs that are managed together, and which communicate using a KeySafe 5 agent. When you load a Security World into an HSM Pool, the Security World will be loaded onto all the HSMs in the HSM pool. The KeySafe 5 agent synchronises the configuration of the HSM pool with all other HSM pools in the Security World. For exam

ple:

- When you create a new Card Set or Softcard (either through KeySafe 5 or manually) on a host machine, it will be synchronised to all HSM pools in the same Security World.
- When you delete a Card Set or Softcard using KeySafe 5, that deletion will be applied by the agent to all HSM pools in the same Security World. However, if you delete a Softcard without using KeySafe 5, that deletion will not be applied to other HSM Pools in the same Security World.

An HSM can only be in one HSM pool at any time unless it is network-connected. However, the HSM can 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.

1.1.4. Security World

Each HSM Pool can make use of a single Security World. Loading a Security World into an HSM Pool will result in that Security World being loaded onto all the HSMs in the pool. A sin gle Security World may be loaded on multiple HSM Pools across many host machines.

For details of Security World use in KeySafe 5, see Security Worlds. For full details of Security World use, refer to the Security World documentation.

1.2. Operations and authorizations

When performing an operation on the command-line, it must be performed in a single step. For example, creating a Security World. Here, all parameters must be specified, all cards inserted, and their passphrases entered.

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. The oper ation is then listed in a list of outstanding operations for the Security World to which it belongs, see Outstanding operations.

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.

Examples:

- 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.
- 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.

1.3. Customer security responsibilities

There are a number of third-party components that are required for correct KeySafe 5 operation, but which are not provided with KeySafe 5. These are considered the responsibility of the customer/operator.

It is the responsibility of the customer to:

- Ensure that the Web Browser contains all the latest security updates from the Web Browser provider.
- Ensure that only authenticated users, that are trusted not to perform malicious actions, are given access to the KeySafe 5 system
- Ensure the integrity of any components that is downloaded from an external source. For example, by verifying the downloaded component using trusted 'hash fingerprints'

or signatures.

- Ensure that a component is updated when an impacting CVE is published for the component.
- Ensure that all components are configured in a secure fashion and deployed in a secure environment.
- Ensure that all third-party components are configured in a secure fashion. For example, all third-party components should use mutually-authenticated secure channels to communicate with the KeySafe 5.
- Ensure that all certificates and keys, used for securing the communications between the third-party components and KeySafe 5, are uncompromised and of sufficient security strength.
- Ensure that the permissions required to access any sensitive configuration items are sufficient. For example, the permissions to access and manipulate a third-party component's server certificates and their associated private key should only be provided to authorised and trusted administrators.
- Ensure that the external identity provider that is providing the bearer token used to authenticate the KeySafe 5 user implements a bearer token with a short lifetime. That is, the bearer token is reissued regularly, as this will mitigate the impact of a compromised bearer token, which would allowing unapproved access to KeySafe 5 for a prolonged period.
- Ensure that a threat analysis of the KeySafe 5 deployed environment has been performed, and that the results of this analysis justify any changes of KeySafe 5 default configuration.

2. The KeySafe 5 Graphical User Interface (WebUI)

2.1. Access the KeySafe 5 WebUI

To access the KeySafe 5 WebUI, in a web browser, navigate to `https://$HOSTNAME`.

The WebUI dashboard provides the following default reports and metrics:

- Outstanding operations
  Pending authorization requests. See Outstanding operations.
- Unhealthy HSMs
- Unhealthy HSM pools
- Unhealthy hosts
- Hardware modules
  HSM distribution by product name.
- Firmware version
  HSM distribution by firmware version.
- Image version
  HSM distribution by image version.
- Security Worlds
  Security World distribution and number of HSM pool assigments.
- HSM pool allocation
  Number of HSMs assigned to each HSM pool.

2.2. KeySafe 5 WebUI notifications

KeySafe 5 WebUI displays notification alerts in the menu bar. To view the notifications, select the **alarm bell** icon.

The following notification types are included:

- Error (red "i")
  Reports that an element of the system is not functioning, and requires immediate atten tion.
- Alert (black triangle)
  Reports that a Monitoring trigger has fired an alert. A hyperlink is typically included to visit the page of the resource.

3. Estate management using the KeySafe 5 WebUI

The following tables provide a quick reference guide to some of the tasks you can perform in KeySafe 5 and how you access the relevant areas of the KeySafe 5 WebUI. These tables are not exhaustive.

3.1. HSM management

Action	Instructions
View HSM information	**Hardware Management** (toolbar) > **HSMs**
Add and manage features	**Hardware Management** (toolbar) > **HSMs** > **Features** (tab)
Delete slot tokens	**Hardware Management** (toolbar) > **HSMs** > **Slots** (tab)
Change mode	**Hardware Management** (toolbar) > **HSMs** > **Basic Information** (tab)
Clear HSM	**Hardware Management** (toolbar) > **HSMs** > **Clear HSM**
Remove HSM record from estate	**Hardware Management** (toolbar) > **HSMs** > **Remove HSM**

3.2. Host machine management

Action	Instructions
View host machine information	**Hardware Management** (toolbar) > **Hosts**
Allocate host machine to pool	**Hardware Management** (toolbar) > **Hosts** > **Move**
Remove host machine from KeySafe 5	**Hardware Management** (toolbar) > **Hosts** > **Delete**

3.3. HSM pools

An HSM Pool is a collection of HSMs that are managed together. Currently, each HSM pool represents one or more host machines.

Action	Instructions
View HSM pool information	**Hardware Management** (toolbar) > **Pools**

Action	Instructions
Create HSM pool	**Hardware Management** (toolbar) > **Pools** (tab) > **Create New Pool**
Allocate HSM pool to Security World	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Pools** (tab) > **Allocate New Pool**
Remove HSM pool from Security World	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Pools** (tab) > **De-Allocate Security World**
Edit HSM pool name	**Hardware Management** (toolbar) > **Pools** (tab) > **Edit Name**
Delete HSM pool	**Hardware Management** (toolbar) > **Pools** (tab) > **Delete**

3.4. Feature certificates

Action	Instructions
View feature certificate information	**Hardware Management** (toolbar) > **Feature Certificates**
Upload feature certificate	**Hardware Management** (toolbar) > **Feature Certificates** > **Upload**

3.5. Security Worlds

Action	Instructions
View Security World information	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]***
Create Security World	**Security Worlds** (toolbar) > **Security Worlds** > **Create New World** Authorize any outstanding operations that were raised, see Outstanding operations.
Edit Security World name	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Edit Name**
Download Security World settings	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Download** Ensure the Security World is not in use before doing this. You can use the downloaded files to configure Security Worlds outside of KeySafe 5 by copying them into the `kmdata` directory on host machines that are not managed by KeySafe 5.
Delete Security World	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Delete** Ensure the Security World is not in use before doing this.

3.6. Cards and card sets

Action	Instructions
Replace Administrator Card Set (ACS)	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Basic** (tab) > **Settings** > **Replace Admin Card Set** You need access to the required number of cards to give permission for the operation and you must have enough blank cards to be used in the new card set. These cards can be new or deleted cards.
Create Operator Card Set (OCS)	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Cards** (tab) > **Create** Authorize any outstanding operations that were raised, see Outstanding operations.
Download OCS	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Cards** (tab) > ***[Card Set name]*** > **Settings** > **Download Card Set** The card set file downloads as a `.zip` file, which contains a separate file for each card.
Change card set passphrase	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Cards** (tab) > ***[Card Set name]*** > **Settings** > **Change Passphrase** Authorize any outstanding operations that were raised, see Outstanding operations.
Delete card set	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Cards** (tab) > ***[Card Set name]*** > **Settings** > **Delete Card Set** You can only delete card sets that are not in use. Deleting a card set using KeySafe 5 deletes all child resources from the KeySafe 5 database. For example, if you are using nShield Web Services, key groups and keys are deleted. This operation does not format the cards. ⚠ Deleting a card set is irreversible.
Create softcard	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Softcard** (tab) > **Create** Authorize any outstanding operations that were raised, see Outstanding operations.
Download softcard	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Softcard** (tab) > ***[Softcard name]*** > **Settings** > **Download Softcard** The Softcard file downloads as a `.zip` file.

Action	Instructions
Change softcard passphrase	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Softcard** (tab) > ***[Softcard name]*** > **Settings** > **Change Passphrase**
Delete softcard	**Security Worlds** (toolbar) > **Security Worlds** > ***[Security World name]*** > **Softcard** (tab) > ***[Softcard name]*** > **Settings** > **Delete Softcard** Deleting a softcard set in KeySafe 5 deletes all child resources from the KeySafe 5 database. For example, if you are using nShield Web Services, key groups and keys are deleted. You can also delete a softcard from a specific slot. ⚠ Deleting a softcard is irreversible.

3.7. Outstanding operations

When a requested task requires authentication, an operation is created. For example, if a card insertion is required for the task, an authentication operation is created. Any operations that have yet to be completed are collectively referred to as outstanding operations.

3.7.1. View outstanding operations

Action	Instructions
View outstanding operations for a specific Security World	**Security Worlds** (toolbar) > **Security Worlds** > **<Security World Name>** > **Operations** (tab)
View Security Worlds with outstanding operations	**Security Worlds** (toolbar) > **Outstanding Operations** Select a Security World to display the outstanding operations.

3.7.2. Approve outstanding operations

You need the relevant physical ACS/OCS cards or virtual softcards and the passphrase to approve outstanding operations. If multiple card authorizations are required, repeat the procedure for each card.

To approve an outstanding operation:

1. Navigate to the outstanding operation, see View outstanding operations.
2. Select **Authorize** to launch the approval wizard.
3. Follow the instructions as directed.

3.7.3. Reject outstanding operations

To reject an outstanding operation:

1. Navigate to the outstanding operation, see View outstanding operations.
2. Select **Reject**.

3.8. Licence management

Action	Instructions
View licence information and system identifier	**Settings** (toolbar) > **Manage Licences**
Upload licence	**Settings** (toolbar) > **Manage Licences** > **Actions** > **Add New Licence**

4. Monitoring WebUI

The following tables provide a quick reference guide to Monitoring functionality in KeySafe 5 and how you access the relevant areas of the KeySafe 5 WebUI. These tables are not exhaustive.

4.1. Trigger management

Action	Instructions
Create Trigger	**Monitoring** (toolbar) > **Alert Configuration** > **Actions** > Add Trigger
Edit Trigger	**Monitoring** (toolbar) > **Alert Configuration** > ***[Trigger]*** > **Actions** > Edit Trigger
Duplicate Trigger	**Monitoring** (toolbar) > **Alert Configuration** > ***[Trigger]*** > **Actions** > Duplicate Trigger
Delete Trigger	**Monitoring** (toolbar) > **Alert Configuration** > ***[Trigger]*** > **Actions** > Delete Trigger

4.2. Alert management

Action	Instructions
View latest alerts	**Bell Icon** (toolbar)
View all alerts	**Bell Icon** (toolbar) > **View all notifications**
Navigate to alerted resource	**Bell Icon** (toolbar) > ***[Alert]*** **Bell Icon** (toolbar) > **View all notifications** > ***[Alert]***
Acknowledge alert	**Bell Icon** (toolbar) > ***[Alert]*** Overflow Menu > **Mark Read** **Bell Icon** (toolbar) > **View all notifications** > ***[Alert]*** Overflow Menu > **Mark Read**
Delete alert	**Bell Icon** (toolbar) > **View all notifications** > ***[Alert]*** Overflow Menu > **Delete** **Note:** Only alerts which have been marked as read can be deleted.

5. Reporting, notifications, and logs

5.1. View KeySafe 5 logs

You can view logs for the central KeySafe 5 platform and the KeySafe 5 Agent from the command line on the KeySafe 5 cluster.

5.1.1. Logs for the central KeySafe 5 platform

The central KeySafe 5 platform application is configured to log to `stdout`. You can view logs by running standard `kubectl` commands.

For example, to get the KeySafe 5 backend services logs:

```
$ kubectl logs -n nshieldkeysafe5 nshield-keysafe5-0 hsm-mgmt
$ kubectl logs -n nshieldkeysafe5 nshield-keysafe5-0 sw-mgmt
```

To get the KeySafe 5 UI logs:

```
$ UI_POD=$(kubectl -n nshieldkeysafe5 get pods -l app=keysafe5-ui-app -o jsonpath='{.items[0].metadata.name}')
$ kubectl logs -n nshieldkeysafe5 $UI_POD
```

Because all logs are directed to `stdout`, you can integrate the application logs with third-party log monitoring tools such as Prometheus or Splunk. This integration is beyond the scope of this document.

5.1.2. Logs for the KeySafe 5 Agent

On Linux-based systems, the KeySafe 5 Agent log file is located at `/opt/nfast/log/keysafe5-agent.log`, unless configured otherwise.

On Windows-based systems:

- The KeySafe 5 agent log file is located at `C:\ProgramData\nCipher\Log Files\KeySafe5-agent.log`, unless configured otherwise.
- The KeySafe 5 Windows Service actions are emitted to the Windows event log under the `nShieldKeySafe5` source identifier.

You can use the `nshieldeventlog` utility to extract these log entries and output them to the console or a text file. For example:

```
nshieldeventlog.exe --source=nShieldKeySafe5
```

As required, specify:

- `-c` | `--count`: The number of records read from the event log.
  The default is `10000`.
- `-f` | `--file`: The output filename.

See the nShield Security World Software documentation for more information on the `nshieldeventlog` utility.

5.2. Resource health measurements

Many of the resource pages in KeySafe 5 include health measurements.

5.2.1. Liveness checks

The central platform receives updates from KeySafe 5 agents on host machines and HSMs. These updates are used to determine how recently the central platform communicated with the resource.

A resource is considered to be "live" if it has been communicated with during a pre-configured *liveness interval*.

For example, if the central platform last communicated with an HSM at 12:00:00 and there is a configured liveness interval of 5 minutes:

- API requests up to 12:05 will have a healthy liveness check
- API requests after 12:05 will have a failing liveness check.

To configure the liveness interval, see the *KeySafe 5 Installation Guide*.

The liveness check behaves according to the following table:

Health Status	Host Agent	Connect Agent
Healthy	Live	Live
	Not Live	Live
Warning	Live	Not Live
Failure	Not Live	Not Live

5.2.2. HSM Management Service

The following health measurements relate to HSM management.

Measurement	Description
liveness	This check passes if the resource has been communicated with during the last health interval. The time returned in the liveness check is the time at which the check was performed. See Liveness checks.
hardwareStatus	This check passes if the hardware status of the HSM is "OK". Check omitted if the HSM does not support reporting its hardware status.
remoteConnectionStatus	This check passes if the remote connection status of the HSM is "OK". Check only valid for Host Health when a Hardserver is configured with a remote module.
hsmQuorum	This check is used for Pool health. • *pass* indicates all HSMs in the Pool are healthy. • *warn* indicates at least one HSM in the Pool is healthy, but not all HSMs in the Pool are healthy. • *fail* indicates all HSMs in the Pool are unhealthy, or there are no HSMs in the Pool.
clockSkew	This check is used for Host health. It passes if the clock on this host is different by no more than the allowed clock skew from the clock on the machine running the HSM Management service. It takes into consideration different time zones between the host machine and the central platform. The allowed clock skew is configurable in the central platform, see the *KeySafe 5 Installation Guide*.

5.2.3. Security World Management Service

The following health measurements relate to Security World management.

Measurement	Description
liveness	This check passes if the resource has been communicated with during the last health interval. The time returned in the liveness check is the time at which the check was performed. See Liveness checks.
poolHealthStatus	This check is used for Authorized Pool health and returns the over all health status of a HSM Pool. This is returned by the HSM Management service API endpoint.
hsmUsableQuorum	This check is used for Authorized Pool health: • *pass* indicates that all HSMs in the Authorized Pool are currently in a "Usable" module state by the Security World that the Pool is authorized to use. • *warn* indicates that at least one HSM in the Pool is not in "Usable" module state. • *fail* indicates that no HSMs in the Pool are in "Usable" module state.

6. Troubleshooting

6.1. Central platform

To view the KeySafe 5 application service logs, see View logs in KeySafe 5.

If a Kubernetes resource is not working as expected, use `kubectl describe` to display any errors with that resource:

```
kubectl describe pod nshield-keysafe5-0
...
Warning  FailedMount  6s (x8 over 70s)  kubelet            MountVolume.SetUp failed for volume "keysafe5-
messagebus-tls-volume" : secret "ks5-amqptls" not found
```

You can also use `kubectl get events` to detect errors:

```
kubectl get events --all-namespaces
```

For more information on debugging Kubernetes applications, see the Kubernetes documentation here.

6.2. KeySafe 5 agent

If the agent fails to start, ensure that the configuration file is present at `%NFAST_DATA_HOME%/keysafe5/conf/config.yaml`.

If the configuration file is present but the agent still fails to start, see the Logging: KeySafe 5 agent section for instructions on accessing the log.

If you are using TLS, ensure that the private key and certificate files are present in `%NFAST_DATA_HOME%/keysafe5/conf/messagebus/tls`.