ENTRUST

KeySafe 5

KeySafe 5 v1.5.0 User Guide

13 November 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.

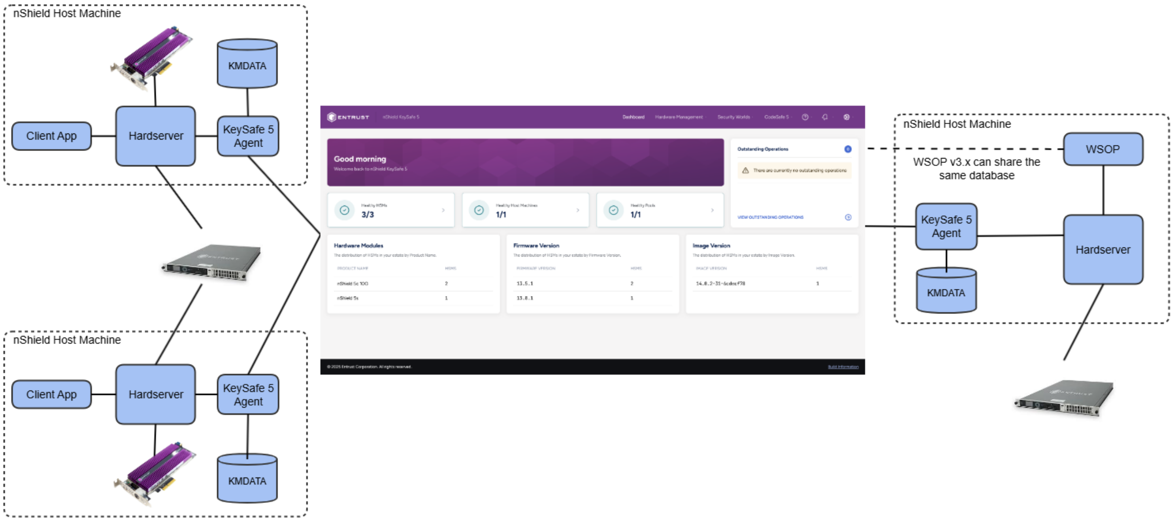
For each nShield host machine that you want to manage using this platform, you must install a KeySafe 5 agent alongside the existing nShield hardserver, see KeySafe 5 Agent Concept. A KeySafe 5 agent is installed on the nShield Connect for nShield Connect images released with Security World v13.4 and later software. This allows KeySafe 5 to manage the nShield Connect without requiring a nShield agent installed on a client machine of the Connect.

For additional information on installing, upgrading, and deploying KeySafe 5, see the *KeySafe 5 Installation and Upgrade Guide*.

2. Deployment Diagrams

A single instance of KeySafe 5 may be used to manage multiple nShield host machines and HSMs. For each host machine/HSM that you want to monitor/manage, you should install and configure a KeySafe 5 agent to connect to the required KeySafe 5 central platform instance.

The KeySafe 5 central platform may be accessed either through the WebUI or the REST API.



3. KeySafe 5 Concepts

3.1. nShield KeySafe 5 agent

On each host machine in your estate that you want to manage with KeySafe 5, the KeySafe 5 agent service is required. The KeySafe 5 agent runs alongside the existing hardserver. The agent communicates the current state of the HSMs / Security World to the central platform and can action management operations for these resources. 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.

3.2. 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.

3.3. 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 example:

- 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.

3.4. HSM Type

KeySafe 5 uses HSM Type to distinguish between the management/monitoring capabilities of different HSM resources in KeySafe 5.

Full HSM

A complete HSM resource capable of most functionality except for creation of Tenancies. For example: nShield 5s, nShield Connect 5c, nShield XC, nShield Connect XC.

Platform HSM

An HSM that manages Tenancies and configuration for the physical module (Only applicable for nShield 5c 10G).

Tenant HSM

An HSM that can perform cryptographic operations but cannot manage Tenancies or configuration of the physical module (Only applicable for nShield 5c 10G).

3.5. 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 single 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.

3.5.1. Security World 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 operation 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.

3.5.2. Resource health measurements

Many of the resources in KeySafe 5 include health measurements.

3.5.2.1. 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

3.5.2.2. 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.

Measurement	Description
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*.

3.5.2.3. 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.

4. The KeySafe 5 REST API

KeySafe 5 provides OpenAPI v3.0 specifications for the RESTful web services that are part of KeySafe 5.

Service	API file in KeySafe 5 release package	Description
Agent Management	api/agent-mgmt.yaml	Management of KeySafe 5 Agents and Central Platform.
CodeSafe Management	api/codesafe-mgmt.yaml	Management of CodeSafe resources.
HSM Management	api/hsm-mgmt.yaml	Management of the nShield Hardware Security Module device. Also, management of Hosts and HSM Pools.
Security World Management	api/sw-mgmt.yaml	Management of the nShield Security World.

You may use tools such as Swagger to generate client SDKs from these OpenAPI Specifica tion definitions.

5. Estate Management

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.

All tasks that described via the KeySafe 5 WebUI may also be actioned directly via the REST API.

5.1. HSMs

5.1.1. HSMs

The table below shows the supported actions for each HSM Type, see HSM Types.

Action	WebUI Location	Full HSM	Tenant HSM	Platform HSM
View HSM information	**Hardware Management** > **HSMs** > **<HSM>**	Y	Y	Y
Manage HSM slots	**Hardware Management** > **HSMs** > **<HSM>** > **Slots**	Y	Y	N
Change mode	**Hardware Management** > **HSMs** > **<HSM>** > **Actions** > **Change Mode** If you change the mode to "Initialization", the HSM will enter the "Pre-initialization" mode until you run **Re-Initialize HSM** in KeySafe 5 (or initunit command in Security World software).	Y	Y	N
Clear HSM	**Hardware Management** > **HSMs** > **<HSM>** > **Actions** > **Clear HSM**	Y	Y	N
Initialize HSM	**Hardware Management** > **HSMs** > **<HSM>** > **Actions** > **Re-Initialize HSM** The HSM must be in "Initialization" or "Pre-initialization" mode before you can initialize it. After ini tializing the HSM, change the mode back to Oper ational.	Y	Y	N
Firmware Upgrade ^More information^	**Hardware Management** > **Firmware Images** **Hardware Management** > **HSMs** > **<HSM>** > **Firmware**	Y	N	Y

Action	WebUI Location	Full HSM	Tenant HSM	Platform HSM
Set Module Minimum VSN ^More information^	**Hardware Management** > **HSMs** > **<HSM>** > **Actions** > **Set (Module) Minimum VSN**	Y	N	Y
Add and manage HSM features ^More information^	**Hardware Management** > **HSMs** > **<HSM>** > **Features** **Hardware Management** > **Feature Certificates**	Y	Y	Y
Remove HSM database record ^More information^	**Hardware Management** > **HSMs** > **<HSM>** > **Actions** > **Remove record**	Y	Y	Y

5.1.1.1. HSM Firmware Upgrade

Firmware files for nShield HSM modules have a .npkg filename suffix.

> ! You can never load firmware with a lower VSN than the target HSM's minimum VSN requirement. For example, if the HSM has a minimum VSN requirement of 3 and the currently installed firmware has a VSN of 4, you can install firmware with a VSN of 3 or above to the HSM. You cannot install firmware with a VSN of 1 or 2 to this HSM.

To upgrade the firmware version of an HSM that is managed via KeySafe 5:

1. Upload the firmware file to KeySafe 5 by navigating to **Hardware Management** > **Firmware Images** and selecting **Actions** > **Upload Firmware Image**.
2. Navigate to the **Firmware** tab of the HSM.
3. On the Firmwares tab, identify the version of HSM firmware that you wish to upgrade to. For this firmware version, click either **Dry Run** (This will check that everything is in place for the upgrade to succeed but will not upgrade the firmware) or **Install**.
4. Carefully check the presented versions are as expected, the click to confirm and start the firmware upgrade.
5. This will create a long-running HSM Operation that you can track to see the progress of the ugprade operation.

When firwmare upgrade is complete the HSM Operation state will be **Complete**.

5.1.1.2. Set HSM Minimum VSN

The version of firmware that can be installed on an HSM is controlled by the Version Security Number (VSN). New firmware being installed must have a VSN value that is equal to, or greater than, the Minimum VSN value. See the *nShield HSM User Guide* for further details.

This setting controls the version of HSM firmware that can be loaded onto a Module. For Connect (Platform) Minimum VSN, see Set Connect Platform Minimum VSN.

The new Minimum VSN value must be higher than the current Minimum VSN value. Once the process has begun, the module will be set to maintenance mode, the minimum VSN will be updated and the module mode will be restored to its previous state. The module will be unavailable for a short period of time while the process completes.

5.1.1.3. Remove HSM record

Removing an HSM record removes the HSM database record from the KeySafe 5 database so that it will no longer appear in KeySafe 5. It does not remove the HSM from the estate.

5.1.1.4. Feature Certificates

Action	WebUI Location
View feature information	**Hardware Management** > **Feature Certificates** > **<Feature>**
Upload and enable feature certificate	**Hardware Management** > **HSMs** > **<HSM>** > **Features** > **Upload New Certificate(s)** **Hardware Management** > **Feature Certificates** > **Actions** > **Upload**

You can order Feature Enabling Certificates from Entrust. They are provided as a text file that you upload to KeySafe 5 from the Feature Certificates page or the Features tab for a specific HSM. The certificates contain the ESN of the HSM for which they were ordered, so you can upload multiple certificates at once and KeySafe 5 assigns them to the appropriate module.

To enable a new feature:

1. Navigate to the **Features** tab of the HSM, or navigate to **Hardware Management** > **Feature Certificates**.
2. On the Features tab, select **Upload New Certificate** or on the Feature Certificates page, select **Actions** > **Upload**.
3. Upload the required certificates, and select **Next Step**.
4. Select **Enable**, and then **Finish and Close Wizard**.

If you finish and close the wizard without enabling the certificate, you can enable it from the Features tab for the relevant HSM.

If a feature does not appear as enabled after uploading the certificate and enabling it, clear the HSM: **Hardware Management** > **HSMs** > **<HSM>** > **Actions** > **Clear HSM**.

You can enable and disable existing feature certificates from the feature information page or on the Features tab for a specific HSM.

For more information about the available features and how to order them, see *Optional features* in the Security World Software documentation.

5.1.2. nShield 5c 10G Platform HSM Management

When you first add an nShield 5c 10G HSM to KeySafe 5, it is added as an HSM resource with HSM Type "Platform", see HSM Types Concept. Platform HSMs are used for managing HSMs using KeySafe 5, not cryptographic or Security World, operations. You must create a tenancy within the HSM, or a "tenant" HSM, to perform cryptographic operations with the HSM.

Action	WebUI Location
Network Configuration ^More information^	**HSM Management** > **HSMs** > **<Platform HSM>** > **Configuration** > **Network**
Time Configuration ^More information^	**HSM Management** > **HSMs** > **<Platform HSM>** > **Configuration** > **Time**
System Logs ^More information^	**HSM Management** > **HSMs** > **<Platform HSM>** > **Information** > **System Logs** **HSM Management** > **HSMs** > **<Platform HSM>** > **Actions** > **Download Logs**
Remote Logging Configuration ^More information^	**HSM Management** > **HSMs** > **<Platform HSM>** > **Configuration** > **Logging**
Tenancy Management ^More information^	**HSM Management** > **HSMs** > **<Platform HSM>** > **Tenancies**
Set Module Minimum VSN ^More information^	**HSM Management** > **HSMs** > **<Platform HSM>** > **Actions** > **Set Module Minimum VSN**
Set Platform Minimum VSN ^More information^	**HSM Management** > **HSMs** > **<Platform HSM>** > **Actions** > **Set Platform Minimum VSN**
Reboot HSM	**HSM Management** > **HSMs** > **<Platform HSM>** > **Actions** > **Reboot**

Action	WebUI Location
Shutdown HSM	**HSM Management** > **HSMs** > **<Platform HSM>** > **Actions** > **Shutdown** ❗ You can not power on the HSM through KeySafe 5. To turn the HSM back on you will need either physical access to the HSM or access to the nShield Connect Serial Console.
Factory State HSM	**HSM Management** > **HSMs** > **<Platform HSM>** > **Actions** > **Factory State** This action will restore the HSM back to its factory state. The HSM will be rebooted as part of this process. ❗ Connectivity to KeySafe 5 will be lost. You must re-configure the Platform KeySafe 5 Agent to communicate with KeySafe 5 once the factory state operation is complete.

5.1.2.1. Network Configuration

Expanding the **Network** card in KeySafe 5 WebUI will show the current network state of the HSM.

- To see the IPv4 Routing Table, select **Routing Table**.
- To see network link information and Small Form-factor Pluggable (SFP) module information for connected SFP modules, select **Link Information**.
- To configure the HSM network, select **Edit**.

See the *nShield Hardware Install and Setup Guides* for further details on the possible network configurations.

5.1.2.2. Time Configuration

Expanding the **Time** card in KeySafe 5 WebUI will show the current time configuration for the HSM.

Setting the time will configure the time on both the HSM platform and the HSM module. To set the time, select **Edit** on the **Time** card. The current time configuration will be displayed. You may either configure the time manually by specifying and exact date/time to use, or you may enable NTP (Network Time Protocol) and configure NTP to synchronize HSM time with an NTP server.

❗ Once you have manually set the time on the HSM at least once, you are

> then unable to set the date and time to a time earlier than the HSM has previously been set to.

In the KeySafe 5 WebUI, the **Information** tab of a Platform HSM resource will show the last 100 lines of platform logs. These logs contain logs of services running on the HSM Platform and the Platform KeySafe 5 Agent running on the platform. If there is a running HSM Tenancy then these logs will also include the hardserver and Tenant KeySafe 5 Agent logs.

To download the last 100,000 lines of platform logs, click the **Download Logs** button. This will download a zip file containing:

- **system.log** The Platform system logs
- **tamper.log** The nShield Connect's Tamper Log is located within the nShield Connect and protected by the nShield Connect's tamper mechanisms. It cannot be erased. See the *nShield Security Manual*.

5.1.2.3. Remote Logging Configuration

Expanding the **Logging** card in KeySafe 5 WebUI will show the current logging configuration for the HSM.

To configure remote logging, select **Edit** on the **Logging** card The current logging configura tion will be displayed. You may enable logging, and configure the IP address and port of the remote syslog server to send platform logs to.

> When configuring the HSM to send logs to a remote syslog server via an IPv6 address, the IPv6 address must be enclosed in square brackets. For example: [1234:2345:3456:4567:5678:6789:789a:89ab]:514

5.1.2.4. Tenancy Management via the Platform HSM

A tenant HSM shares an ESN with the platform HSM to which it belongs, because they both use the same hardware. Creating a tenancy, or a tenant HSM, portions off some of the HSM into a container that has a UUID, known as a "VCM". This means that even though it uses the same hardware, and is a part of the same HSM as the platform, operationally it acts as a separate HSM.

To add a tenant HSM:

1. In KeySafe 5, select **Hardware Management** > **HSMs**, and then select the platform HSM you want to add a tenant to.
   Platform HSMs only have a 12-character ESN in the Identifier column, for example,

AB12-CD34-EF56. Tenant HSMs display the same ESN as their platform HSM as well as their UUID.

2. In the **Tenancies** tab, select **Download CSR**.
   The button is at the bottom of the page.
3. Sign the `certificate.csr` with your PKI infrastructure. See the *KeySafe 5 Installation and Upgrade Guide* for more details.
4. In the **Tenancies** tab, select **Configure**.
   The button is at the bottom of the page.
5. Update the **Central Platform Address** to use the IP address of the KeySafe 5 server.
6. If required, provide a **Name** and toggle the **Auto Start** on.
   Auto start will start the tenancy automatically when the HSM is rebooted. You can manually start the tenancy after configuring it.
7. Upload the `tls.crt` file as the KeySafe 5 Agent Certificate.
   This file might have a different name depending on your signing process.
8. Upload the `ca.crt` file as the CA certificate.
9. Select **Confirm**.
10. When the wizard closes, select **Start** at the bottom of the page.

5.1.2.5. Set Connect Platform Minimum VSN

The version of Connect firmware that can be installed on an HSM is controlled by the Version Security Number (VSN). New firmware being installed must have a VSN value that is equal to, or greater than, the Minimum VSN value. See the *nShield HSM User Guide* for further details.

This setting controls the version of Connect image firmware that can be loaded. For Module (HSM) Minimum VSN, see Set Module Minimum VSN.

The new Minimum VSN value must be higher than the current Minimum VSN value. Once the process has begun, any running tenant will be stopped, the minimum VSN will be updated and the tenant will be restored to its previous state. The module will be unavailable for a short period of time while the process completes.

5.1.3. nShield 5c 10G Tenant HSM Management

Once a Tenant HSM has been configured to communicate with a KeySafe 5 instance, and started, a Tenant HSM resource will appear in KeySafe 5.

This HSM can be configured and used in the same way as earlier models of nShield Connect.

Action	WebUI Location
Dynamic Slots Configuration	**HSM Management** > **HSMs** > **<Tenant HSM>** > **Configuration** > **Dynamic Slots** ℹ The HSM must be cleared for the dynamic slots configuration to take effect.
Slot Mapping Configuration	**HSM Management** > **HSMs** > **<Tenant HSM>** > **Configuration** > **Slot Mapping**
Audit Database Configuration	**HSM Management** > **HSMs** > **<Tenant HSM>** > **Configuration** > **Audit Database Settings**
Hardserver Logs Configuration	**HSM Management** > **HSMs** > **<Tenant HSM>** > **Configuration** > **Hardserver Logs Settings**
Connect Hardserver Configuration	**HSM Management** > **HSMs** > **<Tenant HSM>** > **Configuration** > **Connect Hardserver Settings**
Connect Client Configuration	**HSM Management** > **HSMs** > **<Tenant HSM>** > **Clients**

5.2. Hosts

5.2.1. Hosts

When a host machine is added to KeySafe 5, it is automatically added to a new HSM pool.

Moving a host to a different pool also adds all of its HSMs to that pool.

Action	WebUI Location
View host machine information	**Hardware Management** > **Hosts** > **<Host>**
Allocate host machine to a different HSM pool	**Hardware Management** > **Hosts** > **<Host>** > **Actions** > **Move**
Remove host machine from KeySafe 5 ^More information^	**Hardware Management** > **Hosts** > **Delete**

5.2.1.1. Remove host from KeySafe 5

You can only remove hosts from KeySafe 5 if the host is unhealthy and can not communicate with KeySafe 5. To remove a healthy host, you must first remove the KeySafe 5 agent software from the host.

The HSMs in a removed host machine remain in KeySafe 5, but become unhealthy when they are no longer attached to an agent.

5.3. HSM Pools

5.3.1. HSM pools

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

An HSM pool is automatically created when a new host is added to KeySafe 5. HSM pools are unhealthy if they do not contain any HSMs.

Action	WebUI Location
View HSM pool information	**Hardware Management** > **Pools** > **<Pool>**
Create HSM pool	**Hardware Management** > **Pools** > **Actions** > **Create New Pool**
Allocate a Security World to an HSM pool	**Hardware Management** > **Pools** > **<Pool>** > **Actions** > **Allocate World** **Security Worlds** > **Security Worlds** > **<Security-World>** > **Pools** > **Allocate New Pool** Allocating a Security World to an HSM Pool will create a Security World Operation to load the Security World onto all HSMs in the HSM Pool.
Remove a Security World from an HSM pool	**Security Worlds** > **Security Worlds** > **<Security-World>** > **Pools** > **De-Allocate Security World**
Edit HSM pool name	**Hardware Management** > **Pools** > **<Pool>** > **Actions** > **Edit Name**
Delete HSM pool	**Hardware Management** > **Pools** > **<Pool>** > **Actions** > **Delete**

5.4. Security Worlds

5.4.1. Security Worlds

All nShield HSMs integrate using the nShield Security World architecture.

A Security World contains HSMs, HSM pools, and host machines. It references all associated certificates, licenses, Card Sets, Softcards and operations associated with the Security World.

Before creating a Security World, you must have created an HSM pool for the Security World to be loaded onto, and there must be at least one HSM in that pool.

If a Security World action, for example creation, requires authentication, an outstanding operation is created.

Action	WebUI Location
View Security World information	**Security Worlds** > **Security Worlds** > **<Security World>**
Create Security World	**Security Worlds** > **Security Worlds** > **Actions** > **Create New World**
Edit Security World name	**Security Worlds** > **Security Worlds** > **<Security World>** > **Actions** > **Edit Name**
Download Security World settings ^More information^	**Security Worlds** > **Security Worlds** > **<Security World>** > **Download**
Delete Security World	**Security Worlds** > **Security Worlds** > **<Security World>** > **Delete** Ensure the Security World is not in use before doing this.

5.4.1.1. Use downloaded files to configure Security Worlds not managed by KeySafe 5

> 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.

5.4.2. 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** > **Security Worlds** > **<Security World>** > **Cards** > **Create** Authorize any outstanding operations that were raised, see Outstanding operations.

Action	Instructions
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** > **Security Worlds** > **<Security World>** > **Cards** > ***[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** > **Security Worlds** > **<Security World>** > **Softcard** > **Create** Authorize any outstanding operations that were raised, see Outstanding operations.
Download softcard	**Security Worlds** > **Security Worlds** > **<Security World>** > **Softcard** > ***[Softcard name]*** > **Settings** > **Download Softcard** The Softcard file downloads as a `.zip` file.
Change softcard passphrase	**Security Worlds** > **Security Worlds** > **<Security World>** > **Softcard** > ***[Softcard name]*** > **Settings** > **Change Passphrase**
Delete softcard	**Security Worlds** > **Security Worlds** > **<Security World>** > **Softcard** > ***[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. ⚠ Deleting a softcard is irreversible.

5.4.3. 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.

5.4.3.1. View outstanding operations

Action	Instructions
View outstanding operations for a specific Security World	**Security Worlds** > **Security Worlds** > **<Security World Name>** > **Operations**
View Security Worlds with outstand ing operations	**Security Worlds** > **Outstanding Operations** Select a Security World to display the outstanding operations.

5.4.3.2. 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 pro cedure 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.

5.4.3.3. Reject outstanding operations

To reject an outstanding operation:

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

6. Estate Monitoring

KeySafe 5 supports exporting System, HSM and CodeSafe metrics in OpenMetrics format. This enables integration with external monitoring systems.

The KeySafe 5 metrics endpoints return metrics in OpenMetrics text format (HTTP content-type "application/openmetrics-text"). This format is defined by the OpenMetrics Specification.

The following metric endpoints are available in this release of KeySafe 5.

Endpoint	Minimum KeySafe 5 version	Description	Metric Labels
/system/v1/metrics	1.5	Returns statistics for all known KeySafe 5 Agents and the Central Platform	• agent • type • subject • issuer
/codesafe/v1/metrics	1.2	SEE Machine statistics for all running CodeSafe 5 machines	• uuid (Local machine UUID) • esn • package_name • direction (only applicable to metrics for the network link for an SEE Machine)
/mgmt/v1/hsms/<id>/metrics	1.5	Returns HSM statistics	• esn • label • source • limit • sensor • voltage_sensor • current_sensor • fan_id • vcm

6.1. Integrations

Data from KeySafe 5 metrics endpoints can be imported into any observability tool capable of consuming the OpenMetrics format.

For most tools this consists of configuring your tooling to poll the metrics HTTP endpoint at a certain interval by providing the API endpoint to query along with any necessary authentication.

This section provides basic guidance for a selection of common tools. For more detailed instructions, consult the documentation for your specific tooling.

6.1.1. Prometheus

For Prometheus you must configure a `scrape config` to directly consume the KeySafe 5 metrics data into Prometheus.

An example scrape config for polling an unauthenticated KeySafe 5 CodeSafe metrics endpoint:

```
scrape_configs:
  - job_name: KeySafe 5 CodeSafe
    scrape_interval: 300s
    static_configs:
      - targets: ["example.keysafe5deployment.com"]
    metrics_path: "/codesafe/v1/metrics"
    scheme: https
```

6.1.2. Elastic Stack

Integration with the Elastic Stack (Elasticsearch and Kibana) can be achieved by using the OpenMetrics integration within Kibana. This involves configuring Metricbeat to report the metrics data to Elasticsearch via polling the KeySafe 5 metrics endpoint.

For more details, search for OpenMetrics in Elastic integrations or follow the step-by-step OpenMetrics integration guide within Kibana.

6.1.3. Splunk

For Splunk there is not currently a direct OpenMetrics integration. One possible approach is to configure an HTTP Event Collector and use an intermediary script to poll the KeySafe 5 metrics endpoint, then translate the API responses from KeySafe 5 into a format that can be submitted to the HTTP Event Collector endpoint in Splunk.

6.2. Metrics

6.2.1. Introduction

The following tables display metric exposure in KeySafe 5, the source of the metric, and whether it was available in nShield Monitor or SNMP.

In the tables, the term "resource" refers to whether a statistic belongs to an HSM or a host.

If the statistic belongs to an nShield 5c 10G HSM, the term "resource" also diffentiates between "platform" and "tenancy". All other HSMs report both.

The HSM metrics can apply to the actual HSM ("module") or the HSM "chassis".

6.2.2. OpenMetrics

6.2.2.1. nshield_hsm

The labels on the HSM.

Type	Details
Information	Has the label "label".

6.2.2.2. nshield_error_conditions

Error conditions reported by the 5c 10G chassis. In the 5c 10G, all conditions come from `envmon`.

In non-5c 10G network-attached HSMs, there is only a single error condition available, PSU failure, which comes from `stattree`.

Type	Details	Labels	stattree node	stattree ID	EnvMon
stateset	• failed • okay	source="psu_failed"	`HostEnvStats`	`PSUFailure`	`cosmo_alerts_psu_failed`

6.2.2.3. nshield_uptime_seconds

The length of elapsed time since the HSM was last reset. This does not include the HSM chassis.

Resource	Type	Unit	Details	stattree node	stattree ID	SNMP MIB
Platform	counter	seconds		`ModuleEnvStats`	`Uptime`	`moduleStatsTable` > `uptime`

6.2.2.4. nshield_hsm_liveness

A boolean HSM liveness report where 1 indicates "live".

Resource	Type
Platform	gauge

6.2.2.5. nshield_commands

The total number of commands sent for processing from a client to the server or from the server to an HSM. The number of commands currently being processed is the `CmdCount` minus the `ReplyCount`.

For an HSM, this is the number of commands received from any client.

Resource	Type	Details	stattree node	stattree ID
Tenancy	counter		`ModuleJobStats`	`CmdCount`

6.2.2.6. nshield_replies

The total number of replies sent from a server to a client or from an HSM to a server.

For an HSM, this is the number of replies sent to any client.

Resource	Type	Details	stattree node	stattree ID
Tenancy	counter		`ModuleJobStats`	`ReplyCount`

6.2.2.7. nshield_objects_stored

The number of times the object store has had a new object put into it.

Resource	Type	Details	stattree node	stattree ID
Tenancy	counter		`ModuleObjStats`	`ObjectsCreated`

6.2.2.8. nshield_objects_destroyed

The number of items that have been deleted from the HSM's object store and had their corresponding memory released.

Resource	Type	Details	stattree node	stattree ID
Tenancy	counter		ModuleObjStats	`ObjectsDestroyed`

6.2.2.9. nshield_queue_length_limit

The maximum and minimum queue length. This is a static value obtained from the HSM resource.

Resource	Type	Details
Tenancy	gauge	Has label "limit".

6.2.2.10. nshield_current_clients

The number of client connections currently made to the Connect hardserver.

Resource	Type	stattree node	stattree ID
Tenancy	gauge	`ServerGlobals`	`ClientCount`

6.2.2.11. nshield_current_clients_limit

The number of licensed client connections available.

Resource	Type	stattree node	stattree ID
Tenancy	counter	`ServerGlobals`	`MaxClients`

6.2.2.12. nshield_current_crypto_clients_limit

The number of licenced crypto client connections available.

Resource	Type
Tenancy	gauge

6.2.2.13. nshield_current_crypto_clients

The number of licensable clients that are currently connected, including both active and parked sessions.

This is only relevant when reported from a hardserver with remote clients that have an image version of 13.5 or later.

Resource	Type	stattree node	stattree ID
Tenancy	gauge	`ServerGlobals`	`CryptoClientCount`

6.2.2.14. nshield_audit_db_free_bytes

Resource	Type	Unit	stattree node	stattree ID
Tenancy	gauge	bytes	`ServerGlobals`	`AuditDBFreeSpaceMB`

6.2.2.15. nshield_audit_db_used_bytes

Resource	Type	Unit	stattree node	stattree ID
Tenancy	gauge	bytes	`ServerGlobals`	`AuditDBUsedSpaceMB`

6.2.2.16. nshield_queue_in_progress

All jobs currently in progress on the HSM, including jobs from the SEE machine.

Resource	Type	stattree node	stattree ID
Tenancy	gauge	`ModuleServerStats`	`JobsOutstanding`

6.2.3. System load

6.2.3.1. nshield_cpu_load_per_hsm

The current processing load on the HSM. This is represented as a number from 0 to 100.

HSMs typically contain several different types of processing resources, such as the main CPU and RSA acceleration. This means that reporting on HSM load can be imprecise.

Normally, HSMs report 100% CPU load when all RSA processing capacity is occupied. When performing non-RSA tasks, the main CPU and other resources, such as the random number generator, can become saturated without this metric reaching 100%.

On the nShield Connect, this metric comes from `stattree`.

Resource	Type	Details	Labels	stattree node	stattree ID
Platform	gauge	A value between 0 and 1. Has label "source".	source="module"	`ModuleJobStats`	`CPULoadPercent`
			source="chassis"	`HostEnvStats`	`CPULoadPercent`

6.2.3.2. nshield_cpu_load_average_per_hsm

Resource	Type	Details	Labels	EnvMon
Platform	gauge	A value between 0 and 1. Has label "source".	source="1min"	`cpu_load_average_1min`
			source="5min"	`cpu_load_average_5mins`
			source="15min"	`cpu_load_average_15mins`

6.2.3.3. nshield_cpu_throttled

nShield 5 HSMs only.

An indicator of whether the main processor is being throttled to avoid overheating or not. A throttled processor is confirmation that a module is getting too hot. Processor throttling will impact cryptographic performance.

Resource	Type	Details
Platform	stateset	"throttled" or "okay"

6.2.4. Temperatures

6.2.4.1. nshield_temperature_celsius

The current temperature of different parts of the HSM.

Resource	Type	Units	Details
Platform	gauge	celsius	Has label "sensor".

See the following sections for more details about the labels.

6.2.4.1.1. nshield_temperature_celsius: Module

The current temperature of the main circuit board. First-generation HSMs do not have a temperature sensor and so do not return temperature statistics.

Labels	stattree node	stattree ID
sensor="module_cpu_temp"	`ModuleEnvStats`	`CurrentCPUTemp1`
sensor="module_msp_temp"	`ModuleEnvStats	`TempSP`
sensor="module_crypto_co_proc_temp"	`ModuleEnvStats	`CurrentCPUTemp2`

6.2.4.1.2. nshield_temperature_celsius: Connect (chassis)

The ambient sensors for the chassis.

Labels	stattree node	stattree ID
sensor="chassis_left"	`HostEnvStats`	`CurrentTempC`
sensor="chassis_right"		`CurrentTemp2C`

6.2.4.1.3. nshield_temperature_celsius: 5c 10G (chassis processor)

KeySafe 5 takes the four CPU temperature readings and provides the maximum temperature as the reported value.

Labels	EnvMon
sensor="chassis_processor"	`temp_cpu_core0`
	`temp_cpu_core1`
	`temp_cpu_core2`
	`temp_cpu_core3`

6.2.4.1.4. nshield_temperature_celsius: 5c 10G (inlet and outlet)

The inlet and outlet sensors are similar to the ambient sensors in non-5c 10G network-attached HSMs, however they are in different positions so do not provide the same informa tion.

Labels	EnvMon
sensor="chassis_inlet_left"	`temp_inlet_left`
sensor="chassis_inlet_right"	`temp_inlet_right`
sensor="chassis_outlet_left"	`temp_outlet_left`
sensor="chassis_outlet_right"	`temp_outlet_right`

6.2.4.2. nshield_temperature_limit_celsius

The minimum and maximum acceptable temperature values for each sensor.

For the nShield 5c 10G, these values are provided by the platform. For non-5c 10G network-attached HSMs, these are hardcoded by KeySafe 5.

Resource	Type	Units	Details	Labels
Platform	gauge	celsius	Has labels "sensor" and "limit".	For sensor, see nshield_temperature_celsius limit="maximum"

6.2.4.3. nshield_max_temperature_celsius

The maximum temperature recorded by the HSM's temperature sensor. This is stored in non-volatile memory and is cleared when the unit is initialized.

The `HostEnvStats` are for non-5c 10G network-attached HSMs.

Resource	Type	Units	Details
Platform	gauge	celsius	Has label "sensor".

See the following table for more details about the labels:

Labels	stattree node	stattree ID
sensor="module_cpu_temp"	`ModuleEnvStats`	`MaxTempC`
sensor="chassis_left"	`HostEnvStats`	`MaxTempC`

Labels	stattree node	stattree ID
sensor="chassis_right"	`HostEnvStats`	`MaxTemp2C`

6.2.4.4. nshield_min_temperature_celsius

The minimum temperature recorded by the HSM’s temperature sensor. This is stored in non-volatile memory and is cleared when the unit is initialized.

The `HostEnvStats` are for non-5c 10G network-attached HSMs.

Resource	Type	Units	Details
Platform	gauge	celsius	Has label "sensor".

See the following table for more details about the labels:

Labels	stattree node	stattree ID
sensor="module_cpu_temp"	`ModuleEnvStats`	`MinTempC`
sensor="chassis_left"	`HostEnvStats`	`MinTempC`
sensor="chassis_right"	`HostEnvStats`	`MinTemp2C`

6.2.5. Electrical

6.2.5.1. nshield_platform_voltage_volts

6.2.5.1.1. stattree mapping

Resource	Type	Units	Details
Platform	gauge	volts	Has label "voltage_sensor".

See the following table for more details about the labels:

Labels	stattree node	stattree ID
voltage_sensor="cpu_core"	ModuleEnvStats	CPUVoltage1
voltage_sensor="t1022_ifc_io"		CPUVoltage2
voltage_sensor="t1022_serdes"		CPUVoltage3
voltage_sensor="t1022_serdes_io"		CPUVoltage4
voltage_sensor="fpga_serdes_core"		CPUVoltage5
voltage_sensor="fpga_serdes_io"		CPUVoltage6
voltage_sensor="msp_avcc"		CPUVoltage7
voltage_sensor="ddr4_access"		CPUVoltage8
voltage_sensor="ddr4_io"		CPUVoltage9
voltage_sensor="pci_bus"		CPUVoltage10
voltage_sensor="module_battery"		CPUVoltage11

6.2.5.1.2. EnvMon mapping

Resource	Type	Units	Details
Platform	gauge	volts	Has label "voltage_sensor".

See the following table for more details about the labels:

Labels	EnvMon
voltage_sensor="chassis_battery"	tamper_battery_voltage
voltage_sensor="12V"	power_supply_12V_voltage
voltage_sensor="3V"	
voltage_sensor="5V"	

Labels	EnvMon
voltage_sensor="5VStandby"	`power_supply_5VSB_voltage`

6.2.5.2. nshield_platform_current_amperes

Resource	Type	Units	Details
Platform	gauge	amperes	Has label "current_sensor".

See the following table for more details about the labels:

Labels	EnvMon
current_sensor="12V"	`power_supply_12V_current`
curent_sensor="3V"	
current_sensor="3V"	
current_sensor="5V"	
current_sensor="5VStandby"	`power_supply_5VSB_current`

6.2.6. Fans

6.2.6.1. nshield_fan_speed_rpm

The fan speed for each fan in the HSM.

KeySafe 5 assumes fan speeds greater than 120,000rpm are errors, and instead reports a speed of zero.

Resource	Type	Units	Details
Platform	gauge	rpm	Has label "fan_id".

Labels	stattree node	stattree ID	EnvMon
fan_id="chassis1"	`HostEnvStats`	`CurrentFanRPM`	`fan1_rpm`
fan_id="chassis2"		`CurrentFan2RPM`	`fan2_rpm`
fan_id="chassis3"		`CurrentFan3RPM`	`fan3_rpm`
fan_id="chassis4"		`CurrentFan4RPM`	`fan4_rpm`
fan_id="module"			

6.2.6.2. nshield_fan_speed_limit_rpm

The fan speed limits for each fan in the HSM.

These are hardcoded for each HSM type.

Resource	Type	Units	Details	Labels
Platform	gauge	rpm	Has labels "fan_id" and "limit".	For fan_id, see nshield_fan_speed_rpm. limit = "maximum" and "minimum".

6.2.7. Memory

6.2.7.1. nshield_module_mem_bytes

The total amount of RAM, allocated and free, available to the HSM. This is equal to the installed RAM size, minus various fixed overheads.

It is a static value that is calculated by KeySafe 5.

Resource	Type	Units	stattree node	stattree ID
Platform	gauge	bytes	`ModuleEnvStats`	`MemTotal`

6.2.7.2. nshield_module_mem_alloc_kernel_bytes

The total amount of RAM allocated for kernel use, or non-SEE use, in a module. This is mainly used for the object store, for example, for keys and logical tokens, and for big-number buffers.

Resource	Type	Units	stattree node	stattree ID
Platform	gauge	bytes	`ModuleEnvStats`	`MemAllocKernel`

6.2.7.3. nshield_chassis_mem_alloc_kernel_bytes

The total amount of RAM allocated for kernel use, or non-SEE use, in a module. This is mainly used for the object store, for example, for keys and logical tokens, and for big-number buffers.

Resource	Type	Units	stattree node	stattree ID
Platform	gauge	bytes	`HostEnvStats`	`MemAllocKernel`

6.2.7.4. nshield_module_mem_alloc_user_bytes

The total amount of RAM allocated for user-mode processes in the module. This will be zero for non-SEE use.

This value includes the size of the SEE Machine image and the total heap space available to it. The module's kernel does not know, and therefore cannot report, how much of the user-mode's heap is currently free and how much is in use.

Resource	Type	Units	stattree node	stattree ID
Platform	gauge	bytes	`ModuleEnvStats`	`MemAllocUser`

6.2.7.5. nshield_module_mem_alloc_user_bytes

The total amount of RAM allocated for user-mode processes in the module. This will be zero for non-SEE use.

This value includes the size of the SEE Machine image and the total heap space available to it. The module's kernel does not know, and therefore cannot report, how much of the user-mode's heap is currently free and how much is in use.

Resource	Type	Units	stattree node	stattree ID
Platform	gauge	bytes	`HostEnvStats`	`MemAllocUser`

6.2.7.6. nshield_chassis_virtual_mem_bytes

The total memory in the system.

Resource	Type	Units	EnvMon
Platform	gauge	bytes	`memory_virtual_total`

6.2.7.7. nshield_chassis_virtual_mem_free_bytes

The amount of physical RAM left unused by the system, in kilobytes.

Resource	Type	Units	EnvMon
Platform	gauge	bytes	`memory_virtual_free`

6.2.7.8. nshield_chassis_virtual_mem_available_bytes

An estimate of the amount of memory available for starting new applications without swap ping.

Resource	Type	Units	EnvMon
Platform	gauge	bytes	`memory_virtual_available`

6.2.8. Storage

6.2.8.1. nshield_module_nvram_free_bytes

The total amount of free space in the NVRAM of the HSM.

This is only available on XC and nShield 5 HSM variants.

Resource	Type	Units	stattree node	stattree ID
Platform	gauge	bytes	`ModuleEnvStats`	`NVMFreeSpace`

6.2.8.2. nshield_module_nvram_erase_per_endurance

The wear level of the HSM’s NVRAM, expressed as a percentage of the "erase count:endurance" ratio.

This is only available on XC and nShield 5 HSM variants.

Resource	Type	Details	stattree node	stattree ID
Platform	gauge	A value between 0 and 1	`ModuleEnvStats`	`NVMWWearLevel`

6.2.8.3. nshield_module_worn_blocks_per_nvram

The percentage of worn blocks in the NVRAM of the HSM

This is only available on XC and nShield 5 HSM variants.

Resource	Type	Details	stattree node	stattree ID
Platform	gauge	A value between 0 and 1	`ModuleEnvStats`	`NVMWornBlocks`

6.2.8.4. nshield_chassis_manufacturer_disk_percentage

The percentage used of the storage reserved for manufacturing data.

Resource	Type	Details	EnvMon
Platform	gauge	A value between 0 and 1	`disk_usage_longterm`

6.2.8.5. nshield_chassis_system_disk_percentage

The percentage used of the storage reserved for internal csoftware components.

Resource	Type	Details	EnvMon
Platform	gauge	A value between 0 and 1	`disk_usage_persistent`

6.2.8.6. nshield_chassis_user_disk_percentage

The percentage used of the storage available for user configuration and logs.

Resource	Type	Details	EnvMon
Platform	gauge	A value between 0 and 1	`disk_usage_user`

6.2.9. Internal software statistics

6.2.9.1. nshield_pci_irqs

The number of interrupts from the host. This is approximately equal to the total of `HostReadCount` and `HostWriteCount`.

This is only applicable to PCI HSMs.

Resource	Type	Details	stattree node	stattree ID
Platform	counter		`ModulePCIStats`	`HostIRQs`

6.2.9.2. nshield_pci_unhandled_irqs

The number of unidentified interrupts from the host. If this reports a nonzero value, it is likely that there is a problem with a driver or the PCI bus.

This is only applicable to PCI HSMs.

Resource	Type	Details	stattree node	stattree ID
Platform	counter		`ModulePCIStats`	`HostUnhandledIRQs`

6.2.9.3. nshield_pci_read_reconnect

The number of deferred reads that have now completed. This should be the same as `HostReadDeferred`, or one less than it if there is a currently deferred read.

This is only applicable to PCI HSMs.

Resource	Type	Details	stattree node	stattree ID
Platform	counter		`ModulePCIStats`	`HostReadReconnect`

6.2.9.4. nshield_AIS31_preliminary_alarms

The number of times the AIS31 random number test has failed. Because this test is a statistical test, a small number of failures is expected. If it fails too often, it will trigger a SOS-HRAO alarm and the module will fail.

Resource	Type	Details	stattree node	stattree ID
Platform	counter		`ModuleEnvStats`	`AIS31PrelimAlarms`

6.2.9.5. nshield_correctable_memory_errors

The number of correctable memory errors that have been corrected by the error checking and correction (ECC) mechanisms. Typically, this count should be 0, although a small number of errors are to be expected occasionally. If this count increases rapidly, by multiple thousands per second, there has been a malfunction.

Resource	Type	Details	stattree node	stattree ID
Platform	counter		`ModuleEnvStats`	`MceCount`

6.2.9.6. nshield_spi_communication_attempts

The number of times the main processor on an XC module has had to repeat an attempt to communicate with the security processor due to a communication failure. Loss of communication between the main processor and the security processor cause the module to enter an alarm state and fail. This sometimes triggers an SOS-HV alarm.

Resource	Type	Details	stattree node	stattree ID
Platform	counter		`ModuleEnvStats`	`SpiRetries`

6.2.10. System metrics

6.2.10.1. keysafe5_certificate_expiry

The length of time until the current KeySafe 5 certificate expires.

Type	Unit	Labels
gauge	seconds	agent="agentid"
		type="agent"
		subject="subject"
		issuer="issuer"

7. Troubleshooting

For details on how to obtain logs or troubleshoot either the KeySafe 5 central platform, or a KeySafe 5 Agent, see the *KeySafe 5 Installation Guide*.