KeySafe 5

KeySafe 5 v1.7.0 User Guide

8 April 2026

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
2. Deployment Diagrams . . . 2
3. KeySafe 5 Concepts . . . 3
    3.1. nShield KeySafe 5 agent . . . 3
    3.2. Host Machines . . . 3
    3.3. HSM Pool . . . 3
    3.4. HSM Type . . . 4
    3.5. Security World . . . 4
        3.5.1. Security World Operations and authorizations . . . 4
        3.5.2. Resource health measurements . . . 5
4. Estate Management . . . 8
    4.1. HSMs . . . 8
        4.1.1. HSMs . . . 8
        4.1.2. nShield 5c 10G Platform HSM Management . . . 11
        4.1.3. nShield 5c 10G Tenant HSM Management . . . 14
    4.2. Hosts . . . 15
        4.2.1. Hosts . . . 15
    4.3. HSM Pools . . . 16
        4.3.1. HSM pools . . . 16
    4.4. Security Worlds . . . 16
        4.4.1. Security Worlds . . . 16
        4.4.2. Cards and card sets . . . 17
        4.4.3. Outstanding operations . . . 18
    4.5. Licences . . . 19
5. Estate Monitoring . . . 20
    5.1. Integrations . . . 20
        5.1.1. Prometheus . . . 21
        5.1.2. Elastic Stack . . . 21
        5.1.3. Splunk . . . 21
    5.2. Metrics . . . 21
        5.2.1. HSMs . . . 22
        5.2.2. Hosts . . . 29
        5.2.3. Codesafe . . . 30
        5.2.4. Licensing . . . 31
        5.2.5. System . . . 32
    5.3. Triggers . . . 33
    5.4. Alerts . . . 33

5.4.1. Alert Management . . . 33
5.4.2. Alert Definitions . . . 33
5.4.3. HSM PSU Failure . . . 34
5.4.4. HSM Fan Failure . . . 34
5.4.5. HSM Chassis Battery . . . 34
5.4.6. HSM Fan Speed . . . 35
5.4.7. HSM Memory Usage Percentage . . . 35
5.4.8. HSM Temperature Percentage . . . 35
5.4.9. HSM Queue Percentage . . . 36
5.4.10. HSM Objects Count . . . 36
5.4.11. Host Hardserver . . . 36
5.4.12. HSM Liveness . . . 37
5.4.13. Host Liveness . . . 37
5.4.14. Licence Expiry . . . 37
5.4.15. HSM Client Licences Remaining . . . 38
5.4.16. Certificate Expiry . . . 38
5.5. Alert Notifications . . . 38
5.5.1. WebUI Notifications . . . 39
5.5.2. Email Notifications . . . 39
5.5.3. Webhook Notifications . . . 39
6. Troubleshooting . . . 40

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.

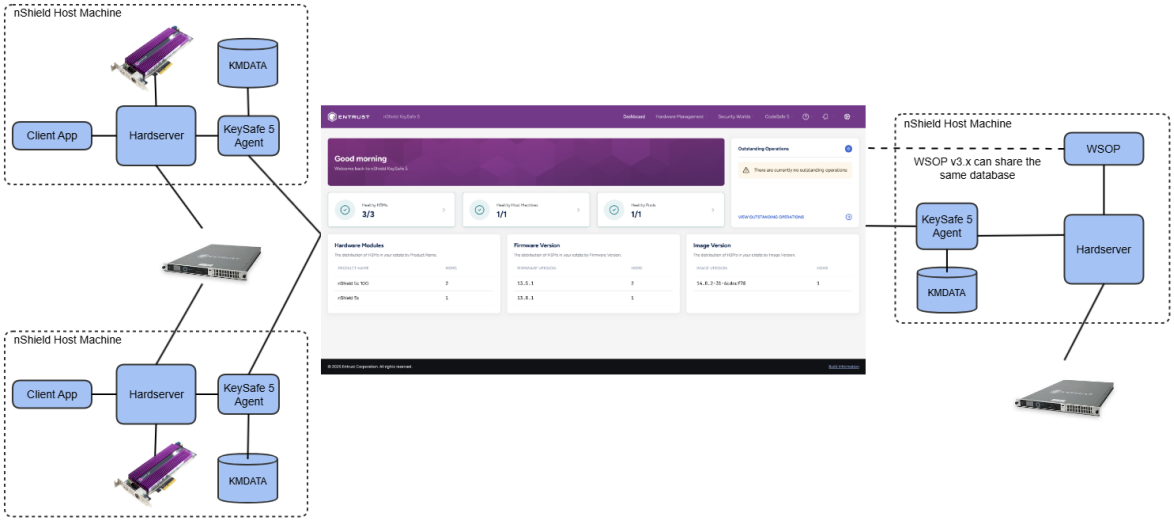
For each nShield host machine that you want to manage using this platform, you must install a KeySafe 5 agent alongside the existing nShield hardserver, see KeySafe 5 Agent Concept. A KeySafe 5 agent is installed on the nShield Connect for nShield Connect images released with Security World v13.4 and later software. This allows KeySafe 5 to man age 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 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.

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.

For liveness interval configuration, see the *KeySafe 5 Installation and Upgrade 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 and Upgrade 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. 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.

4.1. HSMs

4.1.1. 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 initializing the HSM, change the mode back to Operational.	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

4.1.1.1. 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**.

4.1.1.2. 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.

4.1.1.3. 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.

4.1.1.4. 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.

4.1.2. 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.

4.1.2.1. 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.

4.1.2.2. 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*.

4.1.2.3. 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 configuration 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

4.1.2.4. 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.

4.1.2.5. 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.

4.1.3. 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 Con-

nect.

Action	WebUI Location
Dynamic Slots Configuration	**HSM Management** > **HSMs** > **<Tenant HSM>** > **Configuration** > **Dynamic Slots** 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**

4.2. Hosts

4.2.1. 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**

4.2.1.1. 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.

4.3. HSM Pools

4.3.1. 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**

4.4. Security Worlds

4.4.1. 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.

4.4.1.1. 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.

4.4.2. 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.

4.4.3. 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.

4.4.3.1. 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 outstanding operations	**Security Worlds** > **Outstanding Operations** Select a Security World to display the outstanding operations.

4.4.3.2. 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 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.

4.4.3.3. Reject outstanding operations

To reject an outstanding operation:

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

4.5. Licences

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

5. 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

5.1. 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 authenti-

cation.

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

5.1.1. 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
```

5.1.2. 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.

5.1.3. 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.

5.2. Metrics

KeySafe 5 exposes resource metrics in OpenMetrics format. You can pull these metrics into external systems, such as Splunk, to monitor your system.

5.2.1. HSMs

GET /mgmt/v1/hsms/<hsmid>/metrics

Each HSM has a metrics endpoint that reports metrics for that module. Some metrics are available only to specific HSM types.

5.2.1.1. Example

▼ *Details*

```
# TYPE nshield_temperature_limit_celsius gauge
# UNIT nshield_temperature_limit_celsius celsius
# HELP nshield_temperature_limit_celsius The maximum limit of acceptable value for each temperature sensor.
nshield_temperature_limit_celsius{esn="5C95-638E-D5D7",sensor="module_cpu_temp",limit="maximum"} 80
nshield_temperature_limit_celsius{esn="5C95-638E-D5D7",sensor="module_msp_temp",limit="maximum"} 65
nshield_temperature_limit_celsius{esn="5C95-638E-D5D7",sensor="module_crypto_co_proc_temp",limit="maximum"}
80
nshield_temperature_limit_celsius{esn="5C95-638E-D5D7",sensor="chassis_processor",limit="maximum"} 70
nshield_temperature_limit_celsius{esn="5C95-638E-D5D7",sensor="chassis_inlet_left",limit="maximum"} 45
nshield_temperature_limit_celsius{esn="5C95-638E-D5D7",sensor="chassis_inlet_right",limit="maximum"} 45
# TYPE nshield_fan_speed_limit_rpm gauge
# UNIT nshield_fan_speed_limit_rpm rpm
# HELP nshield_fan_speed_limit_rpm The fan speed limits for each fan in the HSM.
nshield_fan_speed_limit_rpm{esn="5C95-638E-D5D7",fan_id="chassis3",limit="minimum"} 8000
nshield_fan_speed_limit_rpm{esn="5C95-638E-D5D7",fan_id="chassis3",limit="maximum"} 18700
nshield_fan_speed_limit_rpm{esn="5C95-638E-D5D7",fan_id="chassis4",limit="minimum"} 8000
nshield_fan_speed_limit_rpm{esn="5C95-638E-D5D7",fan_id="chassis4",limit="maximum"} 18700
nshield_fan_speed_limit_rpm{esn="5C95-638E-D5D7",fan_id="chassis1",limit="minimum"} 8000
nshield_fan_speed_limit_rpm{esn="5C95-638E-D5D7",fan_id="chassis1",limit="maximum"} 18700
nshield_fan_speed_limit_rpm{esn="5C95-638E-D5D7",fan_id="chassis2",limit="minimum"} 8000
nshield_fan_speed_limit_rpm{esn="5C95-638E-D5D7",fan_id="chassis2",limit="maximum"} 18700
# TYPE nshield_platform_voltage_volts gauge
# UNIT nshield_platform_voltage_volts volts
# HELP nshield_platform_voltage_volts The voltage measured on each rail.
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="chassis_battery"} 3.65
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="5VStandby"} 4.9
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="12V"} 11.67
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="t1022_serdes"} 0.9954308
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="fpga_serdes_io"} 4.9255776
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="ddr4_access"} 2.48781168
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="cpu_core"} 0.98584746
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="fpga_serdes_core"} 0.72215104
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="module_battery"} 3.235966
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="t1022_serdes_io"} 1.34002237
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="pci_bus"} 11.6993955
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="ddr4_io"} 1.19293146
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="msp_avcc"} 3.3006072
nshield_platform_voltage_volts{esn="5C95-638E-D5D7",voltage_sensor="t1022_ifc_io"} 1.8039588
# TYPE nshield_AIS31_preliminary_alarms counter
# HELP nshield_AIS31_preliminary_alarms Reports the number of times the AIS31 random number test has failed.
nshield_AIS31_preliminary_alarms_total{esn="5C95-638E-D5D7"} 0
nshield_AIS31_preliminary_alarms_created{esn="5C95-638E-D5D7"} 1769082754
# TYPE nshield_uptime_seconds counter
# UNIT nshield_uptime_seconds seconds
# HELP nshield_uptime_seconds The length of time the HSM has been running.
nshield_uptime_seconds_total{esn="5C95-638E-D5D7"} 361602
nshield_uptime_seconds_created{esn="5C95-638E-D5D7"} 1769082754
# TYPE nshield_module_worn_blocks_per_nvram gauge
# HELP nshield_module_worn_blocks_per_nvram The percentage of worn blocks in the NVRAM of the HSM.
nshield_module_worn_blocks_per_nvram{esn="5C95-638E-D5D7"} 0
# TYPE nshield_temperature_celsius gauge
```

```
# UNIT nshield_temperature_celsius celsius
# HELP nshield_temperature_celsius The temperature of the HSM main circuit board.
nshield_temperature_celsius{esn="5C95-638E-D5D7",sensor="module_msp_temp"} 35
nshield_temperature_celsius{esn="5C95-638E-D5D7",sensor="chassis_inlet_left"} 26
nshield_temperature_celsius{esn="5C95-638E-D5D7",sensor="chassis_processor"} 32
nshield_temperature_celsius{esn="5C95-638E-D5D7",sensor="chassis_inlet_right"} 27
nshield_temperature_celsius{esn="5C95-638E-D5D7",sensor="chassis_outlet_left"} 29
nshield_temperature_celsius{esn="5C95-638E-D5D7",sensor="chassis_outlet_right"} 27.5
nshield_temperature_celsius{esn="5C95-638E-D5D7",sensor="module_crypto_co_proc_temp"} 36
nshield_temperature_celsius{esn="5C95-638E-D5D7",sensor="module_cpu_temp"} 46
# TYPE nshield_module_nvram_erase_per_endurance gauge
# HELP nshield_module_nvram_erase_per_endurance The wear level of the HSM's NVRAM, expressed as a percentage
of the ratio between the erase count and the endurance.
nshield_module_nvram_erase_per_endurance{esn="5C95-638E-D5D7"} 0.003
# TYPE nshield_spi_communication_attempts counter
# HELP nshield_spi_communication_attempts Reports the times the XC Main Processor has had to initiate another
attempt to communicate with the Security Processor due to comms failure.
nshield_spi_communication_attempts_total{esn="5C95-638E-D5D7"} 0
nshield_spi_communication_attempts_created{esn="5C95-638E-D5D7"} 1769082754
# TYPE nshield_max_temperature_celsius gauge
# UNIT nshield_max_temperature_celsius celsius
# HELP nshield_max_temperature_celsius The maximum temperature recorded by the HSM's temperature sensor.
nshield_max_temperature_celsius{esn="5C95-638E-D5D7",sensor="module_cpu_temp"} 48
# TYPE nshield_module_nvram_free_bytes gauge
# UNIT nshield_module_nvram_free_bytes bytes
# HELP nshield_module_nvram_free_bytes The total amount of free space in the NVRAM of the HSM.
nshield_module_nvram_free_bytes{esn="5C95-638E-D5D7"} 2.13598208e+08
# TYPE nshield_module_mem_bytes gauge
# UNIT nshield_module_mem_bytes bytes
# HELP nshield_module_mem_bytes The total amount of RAM (both allocated and free) available to the HSM.
nshield_module_mem_bytes{esn="5C95-638E-D5D7"} 8.304115712e+09
# TYPE nshield_correctable_memory_errors counter
# HELP nshield_correctable_memory_errors Counter reporting the number of correctable memory errors have been
corrected by the onboard error-checking and correction (ECC) mechanisms.
nshield_correctable_memory_errors_total{esn="5C95-638E-D5D7"} 0
nshield_correctable_memory_errors_created{esn="5C95-638E-D5D7"} 1769082754
# TYPE nshield_min_temperature_celsius gauge
# UNIT nshield_min_temperature_celsius celsius
# HELP nshield_min_temperature_celsius The minimum temperature recorded by the HSM's temperature sensor.
nshield_min_temperature_celsius{esn="5C95-638E-D5D7",sensor="module_cpu_temp"} 32
# TYPE nshield_cpu_throttled stateset
# HELP nshield_cpu_throttled Indicates whether the main processor is being throttled to avoid over-heating.
nshield_cpu_throttled{esn="5C95-638E-D5D7",nshield_cpu_throttled="okay"} 1
nshield_cpu_throttled{esn="5C95-638E-D5D7",nshield_cpu_throttled="throttled"} 0
# TYPE nshield_cpu_load_average_per_hsm gauge
# HELP nshield_cpu_load_average_per_hsm The processing load average on the HSM over the time specified by
source.
nshield_cpu_load_average_per_hsm{esn="5C95-638E-D5D7",source="5min"} 8.55
nshield_cpu_load_average_per_hsm{esn="5C95-638E-D5D7",source="15min"} 7.59
nshield_cpu_load_average_per_hsm{esn="5C95-638E-D5D7",source="1min"} 9.98
# TYPE nshield_chassis_system_disk_percentage gauge
# HELP nshield_chassis_system_disk_percentage The percentage used of the storage reserved for internal
software components.
nshield_chassis_system_disk_percentage{esn="5C95-638E-D5D7"} 0.1
# TYPE nshield_chassis_virtual_mem_bytes gauge
# UNIT nshield_chassis_virtual_mem_bytes bytes
# HELP nshield_chassis_virtual_mem_bytes Total memory in the system.
nshield_chassis_virtual_mem_bytes{esn="5C95-638E-D5D7"} 7.9021056e+09
# TYPE nshield_error_conditions stateset
# HELP nshield_error_conditions Error conditions reported by the chassis.
nshield_error_conditions{esn="5C95-638E-D5D7",source="fan2",nshield_error_conditions="okay"} 1
nshield_error_conditions{esn="5C95-638E-D5D7",source="fan2",nshield_error_conditions="failed"} 0
nshield_error_conditions{esn="5C95-638E-D5D7",source="fan3",nshield_error_conditions="okay"} 1
nshield_error_conditions{esn="5C95-638E-D5D7",source="fan3",nshield_error_conditions="failed"} 0
nshield_error_conditions{esn="5C95-638E-D5D7",source="fan4",nshield_error_conditions="okay"} 1
nshield_error_conditions{esn="5C95-638E-D5D7",source="fan4",nshield_error_conditions="failed"} 0
nshield_error_conditions{esn="5C95-638E-D5D7",source="chassis_battery_low",nshield_error_conditions="okay"} 1
```

```
nshield_error_conditions{esn="5C95-638E-D5D7",source="chassis_battery_low",nshield_error_conditions="failed"}
0
nshield_error_conditions{esn="5C95-638E-D5D7",source="fan1",nshield_error_conditions="okay"} 1
nshield_error_conditions{esn="5C95-638E-D5D7",source="fan1",nshield_error_conditions="failed"} 0
nshield_error_conditions{esn="5C95-638E-D5D7",source="psu_failed",nshield_error_conditions="okay"} 1
nshield_error_conditions{esn="5C95-638E-D5D7",source="psu_failed",nshield_error_conditions="failed"} 0
# TYPE nshield_fan_speed_rpm gauge
# UNIT nshield_fan_speed_rpm rpm
# HELP nshield_fan_speed_rpm The fan speed for each fan in the HSM.
nshield_fan_speed_rpm{esn="5C95-638E-D5D7",fan_id="chassis2"} 8939
nshield_fan_speed_rpm{esn="5C95-638E-D5D7",fan_id="chassis3"} 8939
nshield_fan_speed_rpm{esn="5C95-638E-D5D7",fan_id="chassis1"} 8939
nshield_fan_speed_rpm{esn="5C95-638E-D5D7",fan_id="chassis4"} 8939
# TYPE nshield_platform_current_amperes gauge
# UNIT nshield_platform_current_amperes amperes
# HELP nshield_platform_current_amperes The current measured on each rail.
nshield_platform_current_amperes{esn="5C95-638E-D5D7",current_sensor="12V"} 3.17
nshield_platform_current_amperes{esn="5C95-638E-D5D7",current_sensor="5VStandby"} 0.37
# TYPE nshield_chassis_manufacturer_disk_percentage gauge
# HELP nshield_chassis_manufacturer_disk_percentage The percentage used of the storage reserved for
manufacturing data.
nshield_chassis_manufacturer_disk_percentage{esn="5C95-638E-D5D7"} 0
# TYPE nshield_chassis_user_disk_percentage gauge
# HELP nshield_chassis_user_disk_percentage The percentage used of the storage available for user
configuration and logs.
nshield_chassis_user_disk_percentage{esn="5C95-638E-D5D7"} 0.7
# TYPE nshield_chassis_virtual_mem_available_bytes gauge
# UNIT nshield_chassis_virtual_mem_available_bytes bytes
# HELP nshield_chassis_virtual_mem_available_bytes An estimate of how much memory is available for starting
new applications, without swapping.
nshield_chassis_virtual_mem_available_bytes{esn="5C95-638E-D5D7"} 6.499885056e+09
# TYPE nshield_chassis_virtual_mem_free_bytes gauge
# UNIT nshield_chassis_virtual_mem_free_bytes bytes
# HELP nshield_chassis_virtual_mem_free_bytes The amount of memory left unused by the system.
nshield_chassis_virtual_mem_free_bytes{esn="5C95-638E-D5D7"} 5.04612864e+09
# TYPE nshield_hsm_liveness gauge
# HELP nshield_hsm_liveness Whether metrics could be gathered for this HSM.
nshield_hsm_liveness{esn="5C95-638E-D5D7"} 1
# EOF
```

5.2.1.2. Metrics

Some metrics are available only to specific HSM types. In the following table, metrics are described as 'Platform' when they are provided by the hardware and are available to a platform or a full HSM. Metrics described as 'Tenancy' are available to a tenant or to a full HSM. An HSM metric on a Tenant HSM will have a `vcm` label.

Metric	HSM	Type	Unit	Labels	Description
nshield_AIS31_preliminary_alarms	Platform	counter		esn	Reports the number of times the AIS31 random number test has failed.
nshield_audit_db_free_bytes	Tenancy	gauge	bytes	esn, vcm	Free space in the audit database.
nshield_audit_db_used_bytes	Tenancy	gauge	bytes	esn, vcm	Space used in the audit database.

Metric	HSM	Type	Unit	Labels	Description
nshield_chassis_manufacturer_disk_percentage	Platform	gauge		esn	The percentage used of the storage reserved for manufacturing data.
nshield_chassis_mem_alloc_kernel_bytes	Platform	gauge	bytes	esn	Deprecated
nshield_chassis_mem_alloc_user_bytes	Platform	gauge	bytes	esn	Deprecated
nshield_chassis_system_disk_percentage	Platform	gauge		esn	The percentage used of the storage reserved for internal software components.
nshield_chassis_user_disk_percentage	Platform	gauge		esn	The percentage used of the storage available for user configuration and logs.
nshield_chassis_virtual_mem_available_bytes	Platform	gauge	bytes	esn	An estimate of how much memory is available for starting new applications, without swapping.
nshield_chassis_virtual_mem_bytes	Platform	gauge	bytes	esn	Total memory in the system.
nshield_chassis_virtual_mem_free_bytes	Platform	gauge	bytes	esn	The amount of memory left unused by the system.
nshield_commands	Tenancy	counter		esn, vcm	The total number of commands sent for processing from any server to the HSM.
nshield_correctable_memory_errors	Platform	counter		esn	Counter reporting the number of correctable memory errors have been corrected by the onboard error-checking and correction mechanisms.
nshield_cpu_load_average_per_hsm	Platform	gauge		esn, source	The processing load average on the HSM over the time specified by source.

Metric	HSM	Type	Unit	Labels	Description
nshield_cpu_load_per_hsm	Platform	gauge		esn, source	The processing load on the HSM. Because an HSM typically contains a number of different types of processing resources, for example, main CPU and RSA acceleration, this figure is hard to interpret precisely. In general, HSMs report 100% CPU load when all RSA processing capacity is occupied; when performing non-RSA tasks the main CPU or other resources, such as the random number generator, can be saturated without this statistic reaching 100%.
nshield_cpu_throttled	Platform	stateset		esn	Indicates whether the main processor is being throttled to avoid overheating; it will have an impact on crypto performance. Only available on nShield 5 variants.
nshield_current_clients	Tenancy	gauge		esn, vcm	The number of client connections currently made to the hardserver.
nshield_current_-clients_limit	Tenancy	gauge		esn, vcm	The number of licensed client connections available.
nshield_current_crypto_-clients	Tenancy	gauge		esn, vcm	The number of connected remote crypto clients, both active and parked sessions.
nshield_current_crypto_-clients_limit	Tenancy	gauge		esn, vcm	The number of licensed crypto client connections available.
nshield_error_conditions	Platform	stateset		esn, source	Error conditions reported by the chassis.

Metric	HSM	Type	Unit	Labels	Description
nshield_fan_speed_limit_rpm	Platform	gauge	rpm	esn, fan_id, limit	The fan speed limits for each fan in the HSM.
nshield_fan_speed_rpm	Platform	gauge	rpm	esn, fan_id	The fan speed for each fan in the HSM.
nshield_hsm	Platform/Tenancy	info		esn, vcm, label	The labels associated with the HSM.
nshield_hsm_liveness	Platform	gauge		esn	Whether metrics could be gathered for this HSM.
nshield_max_temperature_celsius	Platform	gauge	celsius	esn, sensor	The maximum temperature recorded by the HSM's temperature sensor. This is only cleared when the unit is initialized.
nshield_min_temperature_celsius	Platform	gauge	celsius	esn, sensor	The minimum temperature recorded by the HSM's temperature sensor. This is only cleared when the unit is initialized.
nshield_module_mem_alloc_kernel_bytes	Platform	gauge	bytes	esn	The total amount of RAM allocated for kernel, meaning non-SEE, use in a module. This is principally used for the object store, for example keys and logical tokens, and for big-number buffers.
nshield_module_mem_alloc_user_bytes	Platform	gauge	bytes	esn	The total amount of RAM allocated for user-mode processes in the module. This will be zero for non-SEE use. This includes the size of the SEE Machine image, and the total heap space available to it.
nshield_module_mem_bytes	Platform	gauge	bytes	esn	The total amount of RAM, both allocated and free, available to the HSM.

Metric	HSM	Type	Unit	Labels	Description
nshield_module_nvram_erase_per_endurance	Platform	gauge		esn	The wear level of the HSM's NVRAM, expressed as a percentage of the ratio between the erase count and the endurance. Only available on XC and nShield 5 variants.
nshield_module_nvram_free_bytes	Platform	gauge	bytes	esn	The total amount of free space in the NVRAM of the HSM. Only available on XC and nShield 5 variants.
nshield_module_worn_blocks_per_nvram	Platform	gauge		esn	The percentage of worn blocks in the NVRAM of the HSM. Only available on XC and nShield 5 variants.
nshield_objects_destroyed	Tenancy	counter		esn, vcm	The number of items in the HSM's object store that have been deleted and their corresponding memory released.
nshield_objects_stored	Tenancy	counter		esn, vcm	The number of times a new object has been put into the object store.
nshield_pci_irqs	Platform	counter		esn	On PCI HSMs, the total number of interrupts received from the host.
nshield_pci_read_reconnect	Platform	counter		esn	On PCI HSMs, the number of deferred reads that have now completed.
nshield_pci_unhandled_irqs	Platform	counter		esn	On PCI HSMs, the number of unidentified interrupts from the host. If this is nonzero, a driver or PCI bus problem is likely.
nshield_platform_current_amperes	Platform	gauge	amperes	esn, current_sensor	The current measured on each rail.
nshield_platform_voltage_volts	Platform	gauge	volts	esn, voltage_sensor	The voltage measured on each rail.

Metric	HSM	Type	Unit	Labels	Description
nshield_queue_in_progress	Tenancy	gauge		esn, vcm	The number of jobs that are in progress on the HSM. This value includes all jobs on the module, including jobs from the SEE machine.
nshield_queue_length-_limit	Tenancy	gauge		esn, vcm, limit	queue length (maximum and minimum).
nshield_replies	Tenancy	counter		esn, vcm	The total number of replies returned from HSM to any client.
nshield_spi_communica-tion_attempts	Platform	counter		esn	Reports the times the XC Main Processor has had to initiate another attempt to communicate with the Security Processor due to comms failure.
nshield_temperature_cel-sius	Platform	gauge	celsius	esn, sensor	The temperature of the HSM main circuit board.
nshield_temperature_lim-it_celsius	Platform	gauge	celsius	esn, sensor, limit	The maximum limit of acceptable value for each temperature sensor.
nshield_uptime_seconds	Platform	counter	seconds	esn	The length of time the HSM has been running.

5.2.2. Hosts

`GET /mgmt/v1/hosts/<hostid>/metrics`

Each host resource has a metrics endpoint that reports metrics for that host.

5.2.2.1. Example

▼ *Details*

```
# TYPE nshield_host_liveness gauge
# HELP nshield_host_liveness Boolean Host liveness. (1=live)
nshield_host_liveness{host="4fd93b3a-b09c-43ca-8d89-e76a17808bc4"} 0
# TYPE nshield_hardserver_liveness gauge
# HELP nshield_hardserver_liveness Boolean Hardserver health. (1=live)
nshield_hardserver_liveness{host="4fd93b3a-b09c-43ca-8d89-e76a17808bc4"} 1
# EOF
```

5.2.2.2. Metrics

Metric	Type	Unit	Labels	Description
nshield_audit_db_free_bytes	gauge	bytes	host	Free space in the audit database.
nshield_audit_db_used_bytes	gauge	bytes	host	Space used in the audit database.
nshield_connection_commands	counter		host, connection	The total number of commands sent for processing from a client to the server for each connection.
nshield_connection_replies	counter		host, connection	The total number of replies returned from server to client for each connection.
nshield_current_clients	gauge		host	The number of client connections currently made to the server.
nshield_current_crypto_clients	gauge		host	The number of licensable clients connected, both active and parked sessions.
nshield_hardserver_liveness	gauge		host	Whether the hardserver is considered live (still running).
nshield_host	info		host, label	The labels associated with the host.
nshield_host_connection	info		host, connection, processid, processname	Information about each connection to this host.
nshield_host_liveness	gauge		host	Whether the host is considered live (has sent an update recently).

5.2.3. Codesafe

`GET /codesafe/v1/metrics`

The CodeSafe service provides a single metrics endpoint that returns statistics, where available, for every SEE machine in the Running state. Where metrics cannot be retrieved, they will be omitted.

5.2.3.1. Example

▼ *Details*

```
# HELP codesafe5_cpu_usage_seconds CPU usage in seconds
# TYPE codesafe5_cpu_usage_seconds counter
# UNIT codesafe5_cpu_usage_seconds seconds
codesafe5_cpu_use_seconds_total{uuid="acde070d-8c4c-4f0d-9d8a-162843c10333",esn="1234-5678-
ABCD",package_name="helloworld"} 0
codesafe5_cpu_use_seconds_created{uuid="acde070d-8c4c-4f0d-9d8a-162843c10333",esn="1234-5678-
ABCD",package_name="helloworld"} 1520430000.123
# HELP codesafe5_memory_usage_bytes Mem usage
# TYPE codesafe5_memory_usage_bytes gauge
# UNITS codesafe5_memory_usage_bytes bytes
codesafe5_memory_usage_bytes{uuid="acde070d-8c4c-4f0d-9d8a-162843c10333",esn="1234-5678-
ABCD",package_name="helloworld"} 10000
# HELP codesafe5_kmem_usage_bytes Kmem usage
# TYPE codesafe5_kmem_usage_bytes gauge
# UNITS codesafe5_kmem_usage_bytes bytes
codesafe5_kmem_usage_bytes{uuid="acde070d-8c4c-4f0d-9d8a-162843c10333",esn="1234-5678-
ABCD",package_name="helloworld"} 20000
# HELP codesafe5_link_bytes Information on the link
# TYPE codesafe5_link_bytes counter
# UNITS codesafe5_link_bytes bytes
codesafe5_link_bytes_total{uuid="acde070d-8c4c-4f0d-9d8a-162843c10333",esn="1234-5678-
ABCD",package_name="helloworld",direction="transmit"} 100
codesafe5_link_bytes_created{uuid="acde070d-8c4c-4f0d-9d8a-162843c10333",esn="1234-5678-
ABCD",package_name="helloworld",direction="transmit"} 1520430000.123
codesafe5_link_bytes_total{uuid="acde070d-8c4c-4f0d-9d8a-162843c10333",esn="1234-5678-
ABCD",package_name="helloworld",direction="receive"} 200
codesafe5_link_bytes_created{uuid="acde070d-8c4c-4f0d-9d8a-162843c10333",esn="1234-5678-
ABCD",package_name="helloworld",direction="receive"} 1520430000.123
# EOF
```

5.2.3.2. Metrics

Metric	Type	Unit	Labels	Description
codesafe5_cpu_usage_seconds	counter	seconds	uuid, esn, package_name	CPU usage.
codesafe5_kmem_usage_bytes	gauge	bytes	uuid, esn, package_name	Kmem usage.
codesafe5_link_bytes	counter	bytes	uuid, esn, package_name, direction	Link data transferred reported for both 'receive' and 'transmit'.
codesafe5_memory_usage_bytes	gauge	bytes	uuid, esn, package_name	Memory usage.

5.2.4. Licensing

`GET /licensing/v1/metrics`

The licensing service provides a single metrics endpoint for system licenses.

5.2.4.1. Example

▼ *Details*

```
# HELP keysafe5_licence_expiry The length of time (in seconds) until the licence expires
# TYPE keysafe5_licence_expiry gauge
# UNIT keysafe5_licence_expiry seconds
keysafe5_licence_expiry{licence="Estate Monitoring"} 0
# EOF
```

5.2.4.2. Metrics

Metric	Type	Unit	Labels	Description
keysafe5_licence_expiry	gauge	seconds	licence	The length of time (in seconds) until the licence expires. Currently the only available licence is "Estate Monitoring".

5.2.5. System

Metrics for the system and its agents.

5.2.5.1. Example

▼ *Details*

```
# HELP keysafe5_certificate_expiry The length of time (in seconds) until the certificate expires
# TYPE keysafe5_certificate_expiry gauge
# UNIT keysafe5_certificate_expiry seconds
keysafe5_certificate_expiry{agent="agentid",type="agent",subject="subject",issuer="issuer"} 0
# EOF
```

5.2.5.2. Metrics

Metric	Type	Unit	Labels	Description
keysafe5_certificate_expiry	gauge	seconds	agent, type, subject, issuer	The length of time (in seconds) until the certificate expires. Labels identify the type of certificate ("agent", "central", or "ca") and where the certificate belongs to an agent the id of that agent.

5.3. Triggers

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

5.4. Alerts

5.4.1. Alert Management

Action	WebUI 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.

5.4.2. Alert Definitions

The alerts are listed here by their KeySafe 5 alert type.

The "nShield Monitor Alert" row, where available, indicates that the alert is similar, although not necessarily identical, to a legacy alert from nShield Monitor.

Other data returned

Data marked with "*" are returned only as part of the summary and not as a specific alert record field. For more information about what data is returned, see Labels.

5.4.3. HSM PSU Failure

HSM PSU failed error condition has occurred.

Valid parameters	for
OpenMetrics used	nshield_error_conditions(source="psu_failed")
Other data returned	esn
nShield Monitor alert	NShieldPowerSupplyFailure

5.4.4. HSM Fan Failure

HSM Fan failed error condition has occurred.

Valid parameters	for
OpenMetrics used	nshield_error_conditions(source="fanX")
Other data returned	esn, source*

5.4.5. HSM Chassis Battery

HSM Chassis battery error condition has occurred.

Valid parameters	for
OpenMetrics used	nshield_error_conditions(source="chassis_battery_low")
Other data returned	esn

5.4.6. HSM Fan Speed

The alert is triggered if a fan speed drops below the minimum limit or exceeds the maximum limit.

Valid parameters	for, over
OpenMetrics used	nshield_fan_speed_rpm, nshield_fan_speed_limit_rpm
Other data returned	esn, fan_id
nShield Monitor alert	NShieldXCFanSpeedZero

5.4.7. HSM Memory Usage Percentage

This is the sum of the module kernel and user memory, expressed as a percentage of the total amount of available memory.

Valid parameters	min, max, for, over
OpenMetrics used	nshield_module_mem_bytes, nshield_module_mem_alloc_kernel_bytes, nshield_module_mem_alloc_user_bytes
Other data returned	esn
nShield Monitor alert	memoryUsageHighAlert / memoryUsageOkAlert

5.4.8. HSM Temperature Percentage

The temperature of any sensor, expressed as a percentage of its reported maximum value (calculated from 0°C), is over the specified maximum. The maximum allowed value is 150 percent.

Valid parameters	max, for, over

OpenMetrics used	nshield_temperature_celsius, nshield_temperature_limit_celsius
Other data returned	esn, sensor*
nShield Monitor alert	NShieldTemperaturePeak

5.4.9. HSM Queue Percentage

The percentage of the jobs queue length relative to the job queue limit is under the specified minimum or over the specified maximum value.

Valid parameters	min, max, for, over
OpenMetrics used	nshield_queue_in_progress, nshield_queue_length_limit
Other data returned	esn, vcm
nShield Monitor alerts	DeviceNShieldUtilizationOverloads / DeviceNShieldUtilizationPeakEvent

5.4.10. HSM Objects Count

The number of created objects is under the specified minimum or over the specified maximum value.

Valid parameters	min, max, for, over
OpenMetrics used	nshield_objects_stored_total, nshield_objects_destroyed_total
Other data returned	esn, vcm
nShield Monitor alert	DeviceNShieldHigHObjectCount

5.4.11. Host Hardserver

The host hardserver has failed to communicate recently.

Valid parameters	for
OpenMetrics used	nshield_hardserver_liveness
Other data returned	host
nShield Monitor alert	ClientHostHardserverFailure

5.4.12. HSM Liveness

The HSM has failed to respond and supply metrics.

Valid parameters	for
OpenMetrics used	nshield_hsm_liveness
Other data returned	esn, vcm
nShield Monitor alert	DeviceConnStatus

5.4.13. Host Liveness

The Host has failed to communicate recently.

Valid parameters	for
OpenMetrics used	nshield_host_liveness
Other data returned	host

5.4.14. Licence Expiry

KeySafe 5 licence will expire in less than the specified minimum time.

Valid parameters	min
OpenMetrics used	keysafe5_licence_expiry
Other data returned	licence

5.4.15. HSM Client Licences Remaining

The number of crypto client licences remaining is less than the specified minimum.

Valid parameters	min, for, over
OpenMetrics used	nshield_current_crypto_clients nshield_current_crypto_clients_limit
Other data returned	esn

5.4.16. Certificate Expiry

KeySafe 5 certificate will expire in less than the specified minimum time.

Valid parameters	min
OpenMetrics used	keysafe5_certificate_expiry
Other data returned	type, agent[1]

1. `type` and `agent` values determine which of the following certificates is expiring:
    - Central platform will have type "central" or type "ca" (System certificate, System CA certificate)
    - Agents will have type "agent" or type "ca" but will have an agent id (Agent <agent id> certificate, Agent <agent id> CA certificate)

5.5. Alert Notifications

KeySafe 5 can notify administrators when alerts are triggered through three complementary channels: the WebUI, email, and webhooks. Each method is independent and can be used on its own or in combination.

Notification methods are configured per trigger as *methods*. For details on creating and managing triggers, see Triggers.

5.5.1. WebUI Notifications

The KeySafe 5 WebUI displays alert notifications directly in the browser. No additional configuration is required; notifications appear automatically when alerts are triggered.

Alerts are surfaced via the bell icon in the toolbar, and on the resource page for the specific resource that triggered the alert. For details on viewing, acknowledging, and deleting alerts in the WebUI, see Alerts.

5.5.2. Email Notifications

KeySafe 5 can send alert notifications to a specified email address when an alert is triggered.

To use email notifications, an SMTP server must first be configured. For details on SMTP configuration see the *KeySafe 5 Installation and Upgrade Guide*.

Once the SMTP server is configured, each trigger method can specify a recipient email address to receive notifications for that trigger.

5.5.3. Webhook Notifications

KeySafe 5 can send alert notifications to an external HTTP endpoint when an alert is triggered. This enables integration with third-party systems such as incident management tools.

Webhook notifications are configured per-method on a trigger; each method specifies the target URL that will receive the alert payload.

The webhook payload is sent as an HTTP POST request in JSON format. For details on the payload schema, see the *KeySafe 5 API documentation*.

6. 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 and Upgrade Guide*.