Entrust nShield 5C 10G KeySafe5 Deployment Guide

2026-3-20

© Entrust Corporation. All rights reserved.

Table of Contents

Chapter 1. Introduction

This guide describes:

- How to install and configure Entrust KeySafe 5.
- The procedure to provision a Reconnect Unit on a network.
- The procedure to enroll a client on the Reconnect Unit.
- The procedure to upgrade the Reconnect Unit's firmware.

When these procedures are completed, the combined solution helps support regulatory compliance by applying specific policies and documentation templates to security objects protected in KeySafe 5.

1.1. Product configuration

Entrust has successfully tested Reconnect with Entrust KeySafe 5 in the following configurations:

Product	Version
KeySafe 5	1.5.0
Operating System	Red Hat 9, Windows 2025, Ubuntu 24.04.4
Security World	13.6.14
nShield HSM hardware	nShield 5C 10G
FIPS 140 Level 3	No

1.1.1. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

HSM	Security World Software	Firmware	Image
nShield 5C 10G	13.6.14	13.4.5	14.0.4

Chapter 2. Set Up the KeySafe 5 Server and a Reconnect HSM Unit

2.1. Installing KeySafe 5

Each nShield 5C 10G must be configured on a KeySafe 5 deployment. The KeySafe 5 deployment is used to manage the 5C 10G.

The KeySafe 5 deployment can be on any machine in the same network as the 5c 10G. You will be able to access the 5c 10G via any client that is configured on the 5c 10G.

Skip this section if you already have a compatible KeySafe 5 deployment in place. For compatibility information, see the nShield Security World Release Information

Please refer to the online KeySafe 5 documentation for additional installation instructions:

- KeySafe 5 v1.5 Installation and Upgrade Guide.

For steps on installing Security World software, refer to the online Security World documentation:

- nShield Security World Software v13.6.14 Installation Guide

2.1.1. Server Installation - A quick example

1. Log in to the machine or virtual machine you want to set up as a KeySafe 5 deployment. Update the machine with the latest packages and security patches. If you are using a Linux machine, run the following commands:

   Red Hat 9:

   ```
   % sudo dnf update
   % sudo dnf upgrade
   ```

   Ubuntu :

   ```
   % sudo apt update
   % sudo apt upgrade
   ```

2. Install the Security World software on the KeySafe 5 server.
3. Open up the firewall ports 18080 and 18084:

   RedHat 9 :

```
% sudo firewall-cmd --permanent --add-port=18080/tcp
% sudo firewall-cmd --permanent --add-port=18084/tcp
% sudo firewall-cmd --permanent --add-service=ssh
```

Ubuntu :

```
% sudo ufw allow 18080/tcp
% sudo ufw allow 18084/tcp
% sudo ufw allow ssh
```

Windows :

a. Type Firewall on the Windows search box and open Windows Defender Firewall.
b. Select Advanced settings then select Inbound Rules on the left pane,
c. Select New Rule on the right pane.
d. Select Port, then TCP, and specify local ports.
e. Enter port number 18080 in the text box.
f. Then select Next.
g. Select Allow the connection and Next twice.
h. Enter a name and description, and select Finish. Repeat steps c-g for port 18084.
i. Repeat steps b-g for setting ports 18080 and 18084 in Outbound Rules.

```
An example of Port number and name pair:

Port    Name
18080   KeySafe5Loopback
18084   KeySafe5NATS
```

4. Transfer the `nshield-keysafe5-1.5.0.tar.gz` to the server.
5. Extract the OS-specific content of the file and install it. For example:

Linux :

```
---
% tar xzvf nshield-keysafe5-1.5.0.tar.gz keysafe5-service/keysafe5-server-1.5.0-Linux.tar.gz
% sudo tar xzvf keysafe5-service/keysafe5-server-1.5.0-Linux.tar.gz -C /
% sudo /opt/nfast/keysafe5/server/sbin/install
---
```

Windows :

- Right Click on the `nshield-keysafe5-1.5.0.tar.gz`, select Open.
- Navigate into the `keysafe5-service` folder.
- Run the `keysafe5-server-1.5.0-windows` installer by double-clicking on it.

```
Example installation script output on Linux:

-- Running install fragment keysafe5-server
Creating keysafe5serviced group.
Checking for user 'keysafe5serviced'
Creating keysafe5serviced user.
useradd: warning: the home directory /opt/nfast already exists.
useradd: Not copying any file from skel directory into it.
Checking user 'keysafe5serviced' is in correct group 'keysafe5serviced'
users created correctly
Checking user keysafe5serviced is in group nfast
Initialising...
Detecting all available interface IP addresses that KeySafe 5 agent's may use to connect to the
server.
This list may be manually provided by specifying a comma-separated list of addresses to 'keysafe5-
server-admin init'
The KeySafe 5 internal communication server TLS certificate contains the following addresses that
KeySafe 5 Agents may use to securely connect to the server:
- 127.0.0.1 (loopback/localhost address)
- 10.194.148.22
- ::1 (loopback/localhost address)
- fe80::6e61:6d3a:a0c4:2661
- keysafe5
Generated CA certificate is valid for 30 days
Generated TLS certificates are valid for 30 days
Initialisation complete. You may now add KeySafe 5 Agents using the 'sign' function
Installing startup scripts for 'keysafe5-server'.
Enabling the systemd service unit
Adding and enabling a systemd unit
Created symlink /etc/systemd/system/multi-user.target.wants/nc_keysafe5-server.service →
/etc/systemd/system/nc_keysafe5-server.service.
Starting KeySafe 5 Server
Starting nCipher 'keysafe5-server' server process.
KeySafe 5 Server started
---- Installation complete ----
```

6. Stop and Restart the server:

   Linux :

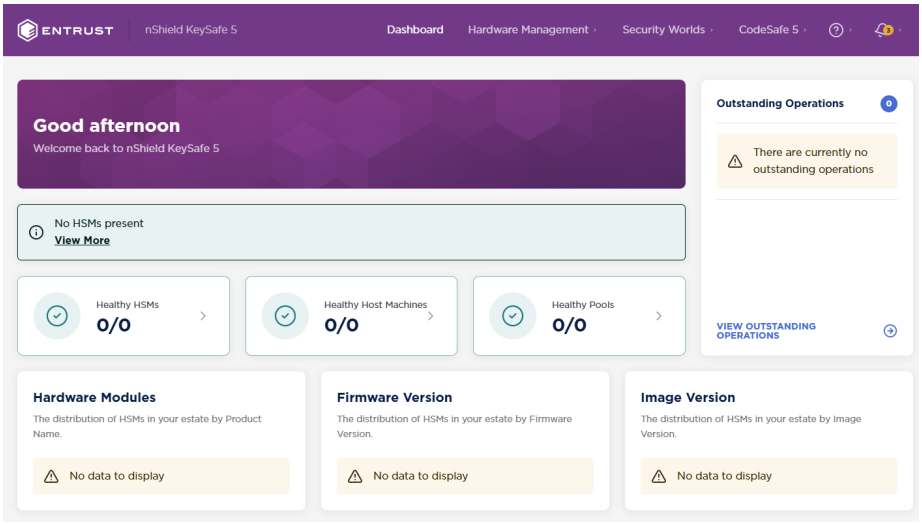
   ```
   % /opt/nfast/scripts/init.d/keysafe5-server stop
   % /opt/nfast/scripts/init.d/keysafe5-server start
   ```

   Windows :

   a. Type Services in the Windows search box, and launch the Services application.
   b. Right click on the `nShield KeySafe 5` service and select Stop, then after it has stopped, click Start.

7. Check that you can access the KeySafe 5 web UI by opening a local browser on the KeySafe 5 server and going to the following address:

   ```
   https://127.0.0.1:18080
   ```



2.2. Setting up the nShield 5C 10G for use as a Reconnect Unit

This section details the steps for installing and configuring an Entrust nShield 5C 10G. For detailed setup procedures and options, see the Security World Software Installation Guide at https://nshielddocs.entrust.com/.

Equipment required for the installation:

- Supplied with the 5c 10G by default:
  - USB serial console cable. To configure the 5C 10G, you must use the serial console through the console port. The serial console port will operate at 115200 baud, 8 data bits, no parity, and 1 stop bit (115200/8-N-1). You can use a serial port aggregator or the serial session software of your choice.
- Supplied with the 5c 10G if ordered:
  - 2x Ethernet port devices: Small Form-factor Pluggable+ module.

You need at least 1 SFP+ module to make the 5c 10G operational.

- NOT supplied with the 5c 10G:
  - KeySafe 5 client-side software (if you have no KeySafe 5 installation yet).
  - 1x host to configure the HSM using the CLI - serial console command line (direct or through a switch).
  - 1x server/VM for the KeySafe 5 installation (optional if you already have installed KeySafe 5).
  - 1x server/VM to act as the client that will use the HSM.

2.2.1. Verifying the physical security of your nShield 5c 10G

See the Physical Security Checklist provided in the box with a 5C 10G, or at https://nshielddocs.entrust.com/.

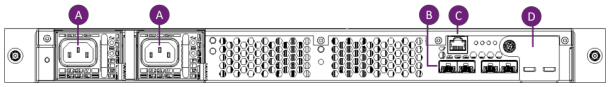
2.2.2. Physically Installing and connecting the HSM module

Please refer to the HSM diagrams in this section in order to identify hardware components present on the HSM when performing the installation.

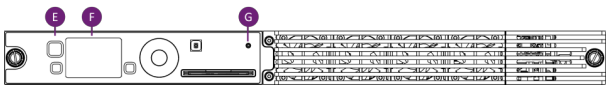
1. Install the nShield 5c 10G in a 19" rack.
    - Follow the instructions supplied with the Entrust nShield® Premium Slide Rail Kit.
2. On the rear of the nShield 5c 10G, plug an SFP+ module into the leftmost SFP+ 10G port, Port 1 (B).
3. Connect the network cable for the main subnet to make the HSM accessible from KeySafe 5.
4. Optionally, if your network settings require the 5c 10G to use additional SFP+ modules, plug them in to the other ports. If your network settings require a secondary subnet, connect a network cable to the relevant SFP+ module.
5. Connect the serial console cable from the serial console port © to the host running your serial session software. The connector can connect directly to your client machine or to a serial port aggregator for remote access.
6. Connect the two power cables to their sockets (A). When connected to power, the nShield 5C 10G will automatically power on.
7. On the front of the 5c 10G, the stand-by button (E) flashes until the boot sequence completes and the details of the boot sequence appear on the screen (F). The status LED (G) shows steady blue after the boot completes and then varies with activity.

HSM rear side:

For your reference, (D) holds the battery for the HSM.



HSM front side:



2.2.3. Identifying the network settings for the nShield 5c 10G

See the 5C 10G network profiles in the nShield Hardware Install and Setup Guide at https://nshielddocs.entrust.com/.

2.2.4. Configuring the network on the nShield 5C 10G

2.2.4.1. Network Transceiver Verification

The nShield 5C 10G supports SFP+ optical ethernet transceiver modules for network connectivity. Using an unsupported transceiver type may result in the interface remaining down, even if IP configuration (IP address, subnet, and gateway) appears correct.

2.2.4.2. Network IP configuration

If you have the HSM connected to a DHCP server, it will automatically set an IP address once network services start if DHCP is enabled.

To configure network settings manually, you must use the HSM serial CLI. This guide includes options to configure IPv4 networking. IPv6 networking is also supported.

1. Open a serial session that connects to the serial cable port interface.
2. Once connected, log in as the cli user.
3. The default password is admin. Change the password when prompted. The new password must be at least 8 characters long.
    - Verify that the serial CLI of the HSM is connected and the console is available. The next steps and commands should be performed on the HSM serial CLI.
4. Set the IP address of the Reconnect Unit on your primary network.

```
(cli)netcfg static -a <5c-10G-ip-addr/prefixlen> -g
```

5. Verify changes with:

```
(cli)netcfg
```

6. Verify network connectivity by pinging the new KeySafe 5 server.

```
(cli)ping <ip-addr-of-ks5-host>
```

2.2.5. Set the Date and Time on the Unit

The date and UTC time on the Reconnect Unit must be the same as the time on the KeySafe 5 Server.

1. Verify the date and time information of the Reconnect unit and the KeySafe 5 server. To check, run the following commands on their respective OS/interface to get current time information.

   Reconnect Unit's Serial CLI :

   ```
   (cli)datetime
   ```

   KeySafe 5 Server (Linux):

   ```
   % date -u +"%Y-%m-%dT%H:%M:%SZ"
   ```

   KeySafe 5 Server (Windows):

   - Open a PowerShell terminal and run the following to get the current time:

     ```
     % [DateTime]::UtcNow
     ```

2. Correct the time information on the Reconnect Unit, if needed, to match the KeySafe 5 server's time. Use the 24-hour clock when updating the Reconnect Unit's time.

   Reconnect Unit's Serial CLI :

   ```
   % (cli)datetime -D <YYYY-MM-DD hh:mm:ss>
   ```

2.2.6. Configure the Reconnect Unit's KeySafe 5 Agent

To configure the KeySafe 5 Agent on the HSM, run the following commands on the Reconnect CLI.

1. Configure the HSM KeySafe 5 agent's `message_bus.url` through the serial CLI. Select `y` when prompted to restart KeySafe 5 agent.

   ```
   (cli)ks5agent cfg message_bus.url=<KeySafe-5-host-IPv4-address>:18084
   ```

   If using IPv6, place square brackets around the address. For example: `(cli)ks5agent cfg message_bus.url=[<KeySafe-5-host-IPv6-address>]:18084`

```
An example output:

(cli)ks5agent cfg message_bus.url=10.194.148.83:18084
logging.level=info
logging.format=json
logging.file.enabled=false
logging.file.path=/opt/nfast/log/keysafe5-agent.log
logging.journal.enabled=true
message_bus.url=10.194.148.83:18084
message_bus.auth_type=tls
message_bus.disable_tls=false
message_bus.minProtocolVersion=TLSV1_2
message_bus.cipherSuites=ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES256-GCM-
SHA384,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-ECDSA-CHACHA20-POLY1305,ECDHE-RSA-CHACHA20-POLY1305
kmdata_network_mount=false
kmdata_poll_interval=1s
update_interval=1m
max_update_message_response_time=1m
health_interval=1m
recovery_interval=5s
codesafe_update_interval=3m
codesafe_cache_period=60m
override_hostname=hsm_64DB-8D35-0405

Restart KeySafe 5 agent to apply new configuration (y|n): y
Restarting KeySafe 5 agent.
Success.
```

2. Verify the configuration with:

```
(cli)ks5agent cfg
```

Chapter 3. Reconnect Procedures

This section describes procedures for managing certificates used by the nShield 5C 10G KeySafe 5 agent, setting up tenancies, and adding clients to the Reconnect Unit's tenancy. These procedures should be performed during initial deployment, certificate renewal, certificate rotation, or recovery scenarios.

3.1. Reconnect KeySafe 5 Agent Certificate Management

3.1.1. Generate a CSR for the HSM KeySafe 5 Agent

Use this procedure to generate a Certificate Signing Request (CSR) for the nShield 5c 10G KeySafe 5 agent. The CSR is generated on the Reconnect Unit using the serial CLI.

1. Run the CSR generation command. The output includes a certificate request block beginning with "BEGIN CERTIFICATE REQUEST" and ending with "END CERTIFICATE REQUEST".

   ```
   (cli)ks5agent mbcsr
   ```

   Example CSR file structure:

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   MIIBvTCCAR8CAQAwITE
   ....
   zSfZvnckFvtRohFOwJv+MEE=
   -----END CERTIFICATE REQUEST-----
   ```

2. Copy the entire certificate request, including the BEGIN and END lines, and save it to a file with a `.csr` extension, for example nShield5c10G.csr.
3. You may optionally verify and display the contents of the CSR to confirm correctness.

   On Linux systems, assuming OpenSSL is installed, use OpenSSL to inspect the CSR.

   ```
   openssl req -in nShield5c10G.csr -noout -text
   ```

   On Windows systems, use OpenSSL to verify the CSR self-signature and display the certificate request details. Successful verification confirms the subject, public key information, extensions, and signature algorithm.

   ```
   openssl req -text -noout -verify -in nShield5c10G.csr
   ```

3.1.2. Signing the CSR

3.1.2.1. Peer-to-peer certificate infrastructure signing

In a peer-to-peer certificate infrastructure, the nShield 5c 10G CSR is signed by the Certificate Authority embedded in the KeySafe 5 application.

1. Log in to the KeySafe 5 server and copy the nShield5c10G.csr file to a directory on the KeySafe 5 server.
2. Execute the CSR signing command using the KeySafe 5 server administration utility. The command outputs Base64-encoded TLS and CA certificates. Examples are provided below for both Linux and Windows environments.

   Linux KeySafe 5 systems:

   ```
   sudo /opt/nfast/bin/keysafe5-server-admin sign nShield5c10G.csr
   ```

   ```
   Example output:

   user@keysafe5:~/Downloads/new$ sudo /opt/nfast/bin/keysafe5-server-admin sign nShield5c10G.csr
   Base64 encoded tls.crt:
   LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNkekNDQVlxZ0F3SUJBZ0lCQ0RBS0....VPaVBmcEcvMmszQllsVW9hOUNvb2RTMUg
   KLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQo=

   Base64 encoded ca.crt:
   LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWFXZ0F3SUJBZ0lCS2pBS0....TRVhXQmFlT0pPCmF4VHhPUWFXUC9vPQot
   LS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==

   Successfully signed CSR nShield5c10G.csr for 30 days
   Saved certificates tls.crt and ca.crt in the current directory
   ```

   Windows KeySafe 5 Systems:

   ```
   "C:\Program Files\nCipher\nfast\bin\keysafe5-server-admin.exe" sign nShield5c10G.csr
   ```

   ```
   An Example output:

   C:\Users\Administrator.INTEROP\Documents\certificates-ks5ca-signed>"C:\Program
   Files\nCipher\nfast\bin\keysafe5-server-admin.exe" sign nShield5c10G.csr
   Base64 encoded tls.crt:
   LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNLRENDQVlxZ0F3SUJBZ0lCQXpBS0....YYXpqMVozM0hXODZzWlp2cXJMMGxtdz09
   Ci0tLS0tRU5EIENFUlRJRklDQVRFLS0tLS0K

   Base64 encoded ca.crt:
   LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWFXZ0F3SUJBZ0lCS2pBS0....UUWhZTUVvaHQrCnlrVnA0WmhKbDZzPQot
   LS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==

   Successfully signed CSR nShield5c10G.csr for 30 days
   Saved certificates tls.crt and ca.crt in the current directory
   ```

- The output confirms successful signing, displays the Base64-encoded certificate strings, and indicates that the certificate files have been saved in the current directory.

Copy the Base64 encoded strings for the tls.crt and ca.crt for later use.

3.1.3. Install the Signed Certificates on the nShield 5c 10G

1. Install the TLS certificate on the nShield 5c 10G by providing the Base64-encoded TLS certificate string through the CLI with the following command. The CLI will confirm that the certificate data has been saved successfully.

```
(cli)ks5agent mbtls tls.crt <Base64-encoded-TLS-string>
```

```
An example:

(cli)ks5agent mbtls tls.crt LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tC...

Saved Base64 encoded data to tls.crt.
```

2. Install the CA certificate on the nShield 5c 10G by providing the Base64-encoded CA certificate string through the CLI with the following command. The CLI confirms that the certificate data has been saved successfully.

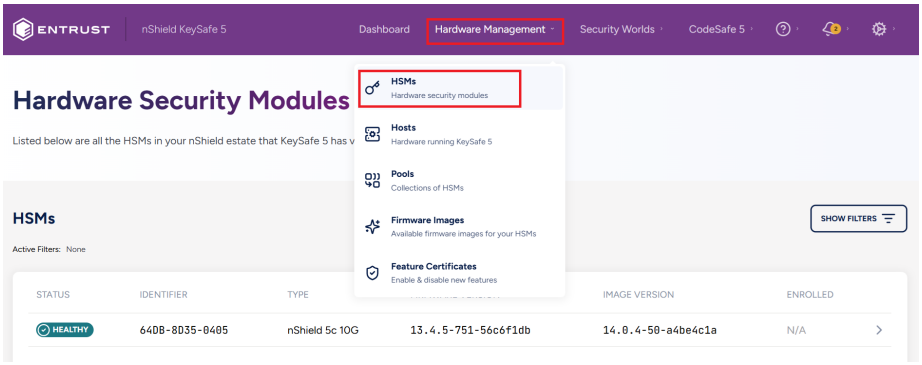
```
(cli)ks5agent mbtls ca.crt <Base64-encoded-CA-string>
```

```
An example:

(cli)ks5agent mbtls ca.crt LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JS...

Saved Base64 encoded data to ca.crt.
```

3. Restart the nShield 5c 10G KeySafe 5 agent to apply the newly installed certificates. A successful restart confirms that the updated configuration has been loaded.

```
(cli)ks5agent restart
```

4. Next, verify the HSM's state. From the KeySafe 5 User Dashboard, click Hardware Management, then HSMs. Confirm that the HSM status is shown as HEALTHY. Please refer to the Troubleshooting section later in this guide if the HSM does not appear in the GUI.

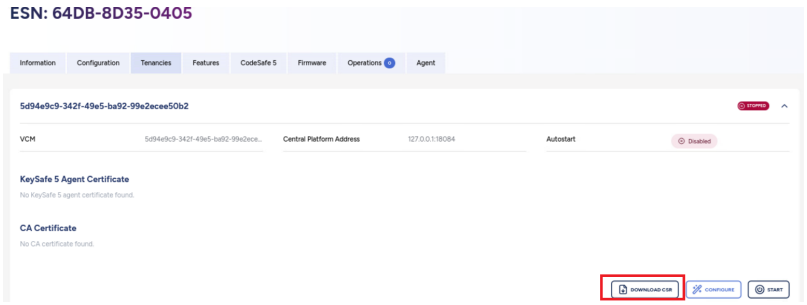


3.2. Creating a Tenancy and Adding Clients

3.2.1. Setting up a Tenancy

To enable access to the HSM from KeySafe 5, a tenancy must be set up on the HSM.

1. From the KeySafe 5 Dashboard, navigate to Hardware Management > HSMs. Select your HSM to proceed.
2. Select the HSM's Tenancies Tab, and then click the Download CSR button at the lower right corner of the screen.



3. Transfer the downloaded `certificate.csr` to the KeySafe 5 Server, and perform the signing operation on it.

> In the example output, the signed certificate was given a custom validity period of 2 years. See the section titled Additional Information later in this guide for more details.

Linux KeySafe 5 Systems :

```
sudo /opt/nfast/bin/keysafe5-server-admin sign certificate.csr 730
```

```
Example output:

user@keysafe5:~/Downloads/tenancy$ sudo /opt/nfast/bin/keysafe5-server-admin sign certificate.csr 730
```

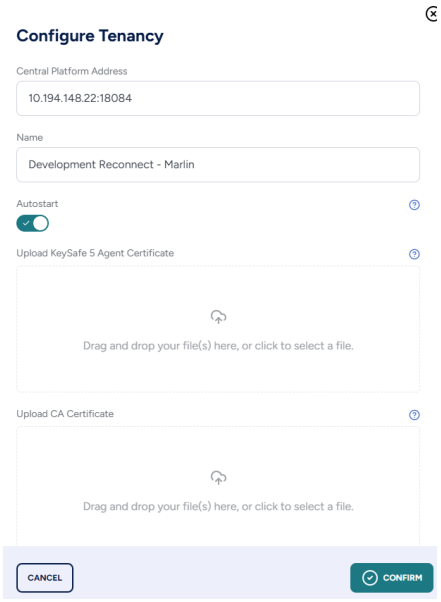
```
Base64 encoded tls.crt:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNkRENDQWRhZ0F3SUJBZ0lCQ1RBS0....FGck5UWFBzaU10Y08KeTRYY0hGMzBwSUU
9Ci0tLS0tRU5EIENFUlRJRklDQVRFLS0tLS0K

Base64 encoded ca.crt:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWFXZ0F3SUJBZ0lCS2pBS0....dTRVhXQmFlT0pPCmF4VHhPUWFXUC9vPQo
tLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==

Successfully signed CSR certificate.csr for 730 days
Saved certificates tls.crt and ca.crt in the current directory
```

Windows KeySafe 5 Systems:

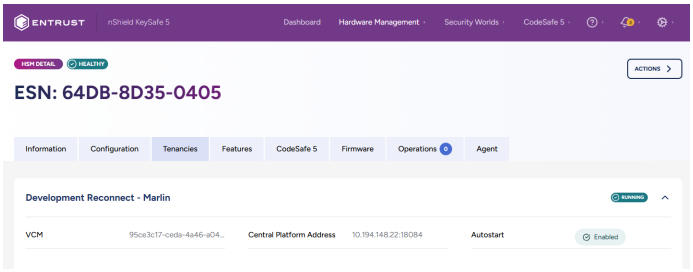
```
"C:\Program Files\nCipher\nfast\bin\keysafe5-server-admin.exe" sign certificate.csr 730
```

```
An Example output:

C:\Users\Administrator.INTEROP\Downloads>"C:\Program Files\nCipher\nfast\bin\keysafe5-server-admin.exe"
sign certificate.csr 730
Base64 encoded tls.crt:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNkRENDQWRhZ0F3SUJBZ0lCQmpBS0....tZYnpOQUxzaGJuemcKcmYzSW5GdDNQUjQ
9Ci0tLS0tRU5EIENFUlRJRklDQVRFLS0tLS0K

Base64 encoded ca.crt:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNSRENDQWFXZ0F3SUJBZ0lCS2pBS0....NUUWhZTUVvaHQrCnlrVnA0WmhKbDZzPQo
tLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==

Successfully signed CSR certificate.csr for 730 days
Saved certificates tls.crt and ca.crt in the current directory
```

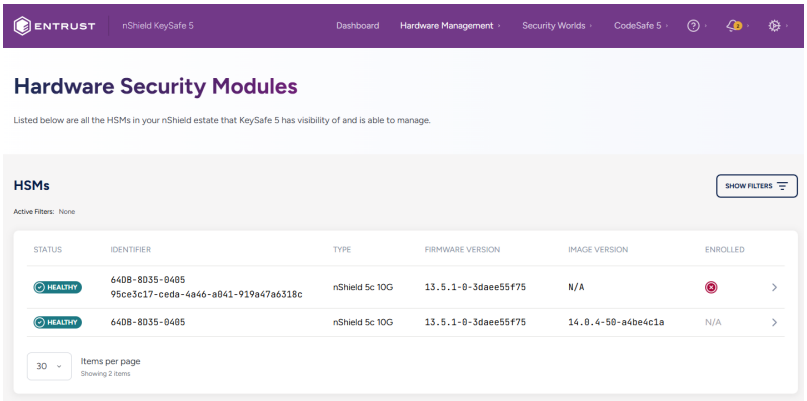
4. In the KeySafe 5 Web GUI, select your HSM. Click the Tenancies tab, then click Configure in the lower-right corner. Input the following information in the Configure Tenancy Window:
   a. Input the Central Platform IP address which is your KeySafe 5 server IP address.
   b. Input a Name for the Tenancy.
   c. Select Autostart.
   d. Upload the signed tls.crt and ca.crt generated by the signing operation in the previous step.



5. Select Confirm on the Configure Tenancy Window, then close.
6. Select Start at the lower right corner of the HSM's Tenancy Tab. Select Confirm to start the Tenancy.
7. Verify that the created Tenancy appears in the HSM's Tenancy Tab.



8. At Hardware Management > HSMs, you should see two HSMs with the same ESN. The HSM entry with the VCM visible as an Identifier is the Tenant HSM while the other entry is the platform HSM. Verify that the tenant HSM is available and Healthy.



3.2.2. Client Configuration

3.2.2.1. Adding Clients to the Tenancy

For a client to access and use the HSM for security purposes, the client must be added to the HSM's tenancy.

1. On the Client that will be added to the HSM tenancy, install the latest version of the Security World software as described in the Installation Guide for the HSM. Ensure the Security World software is installed and operational before proceeding.
2. On the Client, run the following command and save the kneti hash.

```
% sudo /opt/nfast/bin/enquiry
```

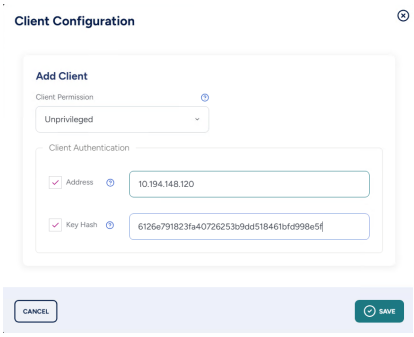
```
For example:

[root@ocp4-redhat-9 ~]# /opt/nfast/bin/enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number
 mode                 operational
 version              13.6.14
...
 remote port (IPv4)   9004
 kneti hash           6126e791823fa40726253b9dd...
 rec. LongJobs queue  0
...
```

3. In the KeySafe 5 Web GUI, navigate to Hardware Management > HSMs. Select the Tenant HSM, then select the Clients tab.
4. Select Add New Client, which will bring up the Client Configuration window. Input the following information.
   a. Select the intended Client Permission type. By default, this is set to Unprivileged.
   b. In the Client Authentication area, consider the following options when making your selection:

Address Box	KNETI Hash Box	Instruction/Purpose
Checked	Unchecked	Enter the client's IP address. Any client with that IP address will be allowed to use the HSM irrespectively of its KNETI hash.
Unchecked	Checked	Enter the client's KNETI hash. Any client with that KNETI hash will be allowed to use the HSM regardless of its IP address.

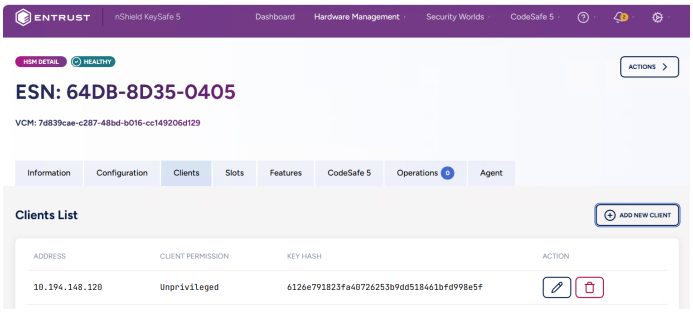
Address Box	KNETI Hash Box	Instruction/Purpose
Checked	Checked	Enter both the client's IP address and KNETI hash. These need to match to allow the client to use the HSM.

- An example selection:

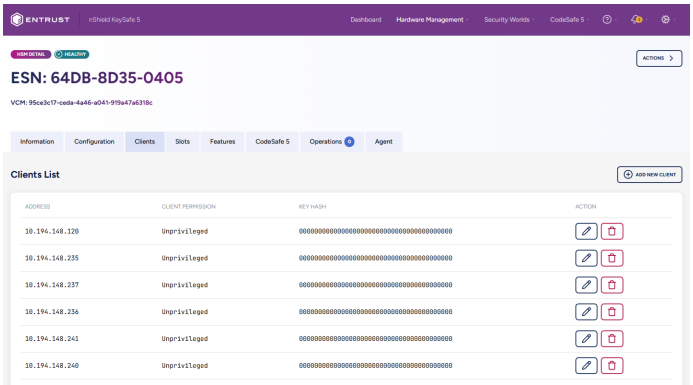


c. Select Save and then Close. It may take a few seconds before the Client appears in the Web GUI.

5. Once the Client appears in the Client List, the HSM is ready to be used by the Client.



Example of multiple clients added with KNETI hash unchecked:



3.2.2.2. Enrolling the HSM in the Client's Security World

1. On the Client machine, run the following Security World utility command to determine the Electronic Serial Number (ESN) and KNETI hash of the HSM to enroll. Input the HSM's IP address in the field designated by `<HSM-IP-address>`.

```
% sudo /opt/nfast/bin/anonkneti <HSM-IP-address>
```

2. Enroll the HSM with the Security World utility command `nethsmenroll`. Two methods are available.
   a. Using the HSM IP address. You will be prompted to validate the ESN and HASH in order to do the enrollment.

```
% sudo /opt/nfast/bin/nethsmenroll <HSM-IP-address>
```

   b. Using the ESN and KNETI Hash, specifying privileged or keeping the default unprivileged connection type.

   Privileged connection :

```
% sudo /opt/nfast/bin/nethsmenroll --privileged <HSM-IP-address> <HSM-ESN> <HSM-kneti-hash>
```

   Unprivileged connection:

```
sudo /opt/nfast/bin/nethsmenroll <HSM-IP-address> <HSM-ESN> <HSM-kneti-hash>
```

3. Check that the HSM has been enrolled. The HSM should be listed in the module section of the output (e.g. Module #1). The mode should be operational, and the hardware status should be OK.

```
% sudo /opt/nfast/bin/enquiry
```

```
An Example output:

[root@ocp4-redhat-9 ~]# enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        ...
 mode                 operational
 version              13.6.14
...

Module #1:
 enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        ...
 mode                 operational
 version              13.4.5
```

```
...
 module type          nShield 5c 10G
...
 hardware status      OK
```

4. The HSM is now able to be used by the Client machine for security purposes.

3.3. Additional Procedures

This section describes optional or infrequently performed procedures that may be required in specific operational scenarios. These actions are not part of standard setup or day-to-day operation but are provided for advanced configuration, maintenance, or troubleshooting purposes.

3.3.1. Modifying Signed Certificate Validity Periods

By default, signed certificates are valid for 30 days. To extend the validity period, you can either change the CA validity period on the KeySafe 5 server for all signings, or specify a custom validity period for an individual CSR signing operation.

Commands shown below are to be run on the KeySafe 5 server.

- Changing the CA validity on the KeySafe 5 server for all signings, for example, to 730 days (2 years):

```
/opt/nfast/bin/keysafe5-server-admin init -y --ca 730 --server 730
```

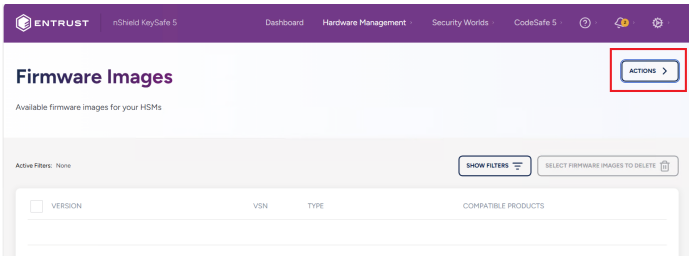
- Changing the validity period for a single CSR signing to a custom period:

```
sudo /opt/nfast/bin/keysafe5-server-admin sign nShield5c10G.csr 730
```

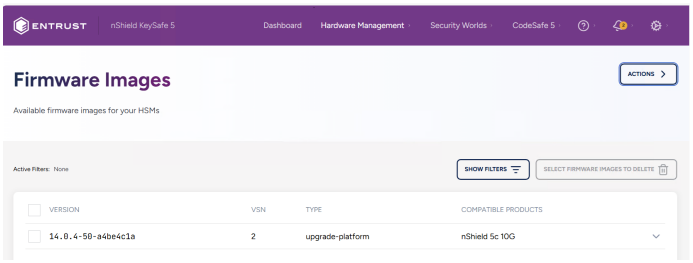
3.3.2. Upgrading the Reconnect Unit's Firmware through KeySafe 5

3.3.2.1. Upload the Firmware to KeySafe 5

1. Download the firmware package for your HSM, and extract the compressed file with the extension `.npkg`
2. In the KeySafe 5 Web GUI, navigate to Hardware Management > Firmware Images.
3. Select the Actions button at the upper right corner.



4. In the Upload HSM Firmware Image window, drag and drop or upload the firmware upgrade file.
5. Select Upload Image. A confirmation window will appear with the firmware's details. Click close once you are done verifying.
6. The Firmware Images window should now have an entry with your uploaded firmware.

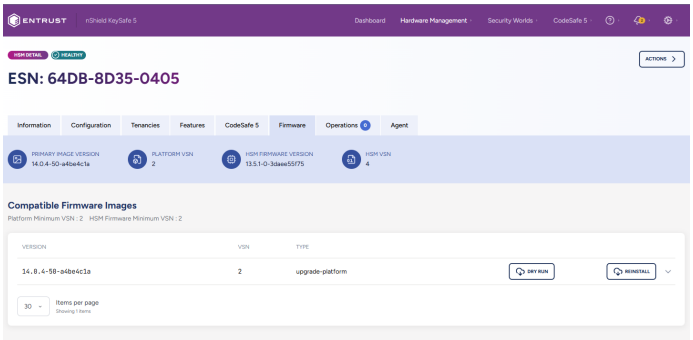


3.3.2.2. Performing the Firmware upgrade

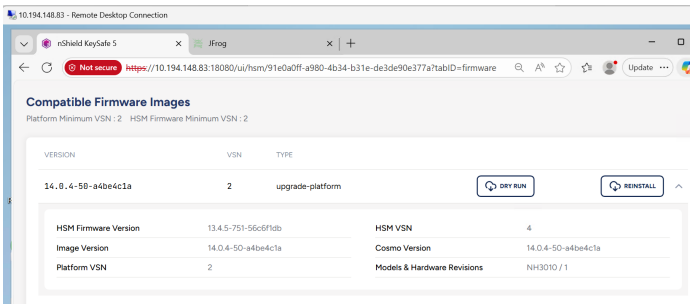
1. Once the firmware package is available in the KeySafe 5 GUI, navigate within the GUI to Hardware Management > HSMs.
2. Select the Platform HSM you wish to upgrade.

> The Platform HSM will not have a VCM visible as its identifier, while the Tenant HSM does. Ensure the Platform HSM is the one selected.

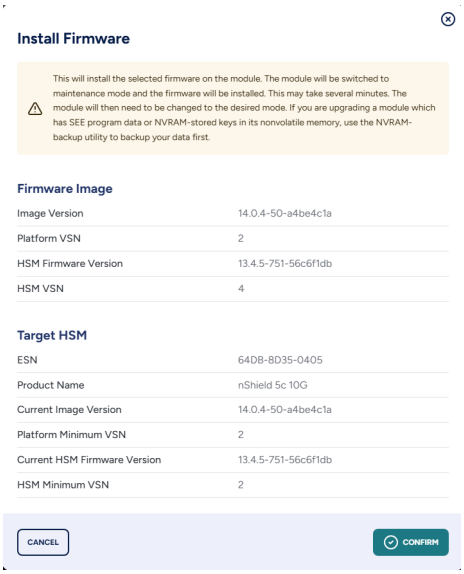
3. Select the HSM's Firmware tab. Here you can verify the HSM's current firmware version, and any compatible firmware versions you can upgrade to.



4. Select the version of firmware you wish to upgrade the HSM to. Verify the firmware package's details.

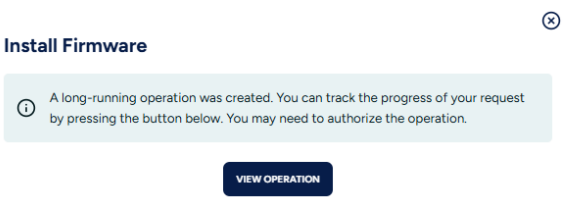


5. Select the Reinstall button to install the selected firmware version package. A menu will open so you may verify firmware compatibility with your HSM.



6. Select Confirm to proceed.
7. An Install Firmware dialog window will appear, allowing you to optionally view the progress of the installation.

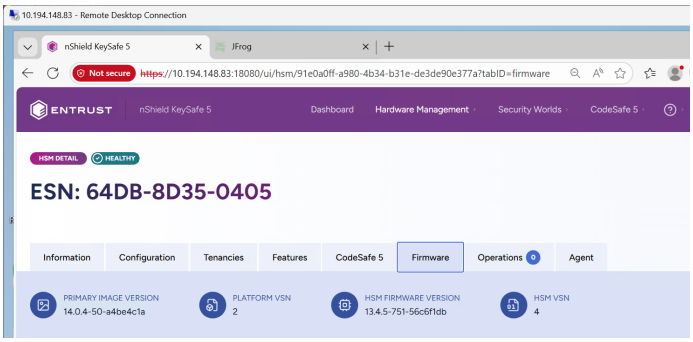
> Although an Upgrade Successful message appears during the install, it may take up to 10 minutes for the upgrade to successfully complete.



8. To verify that the firmware package installed successfully, navigate to Hardware Management > HSMs in the KeySafe 5 Web GUI and select the Platform HSM where

you installed it.

9. When you select the firmware tab of the HSM, you will be able to see the new firmware version under the HSM Firmware Version field.



Chapter 4. Troubleshooting

This section provides guidance for diagnosing and resolving common issues that may be encountered during the installation, configuration, or operation of the Reconnect HSM or KeySafe 5 system.

4.1. Interface link remains down after network configuration

1. Verify the network configuration:

   ```
   (cli)netcfg
   ```

   - Confirm that:
     - The gateway address is present and correct.
     - The subnet mask matches the network.
2. If the gateway and IP configuration are correct and the interface status remains down, inspect the physical network connection.

   ```
   Example output showing link-down status:

   (cli)netstatus
   Active Profile: SINGLE
   Interface: Management (eno1)
   MAC: 00:60:e0:b3:eb:51
   Status: down
   Addresses:
   IP: 10.X.X.X/24
   Scope: 0
   Broadcast: 10.X.X.X
   Cfg Source: static
   ```

3. Verify the type of transceiver installed in the associated port.

The nShield 5C 10G device supports SFP+ transceivers. It does not support SFP-T transceivers.

4.2. nShield 5C 10G not appearing in KeySafe 5 Web GUI

1. Review the KeySafe 5 agent logs by executing the following command in the HSM's CLI. Successful logs indicate agent startup, configuration updates, and successful message bus connectivity.

```
(cli)ks5agent log
```

```
An example of agent logs showing successful connection:

Dec 10 19:04:32 nshield-64DB-8D35-0405 audit[158675]: SYSCALL arch=c000003e syscall=257 success=no exit=-13
a0=ffffffffffffff9c a1=772642228753 a2=80000 a3=0 items=0 ppid=158652 pid=158675 auid=4294967295 uid=100006
gid=100001 euid=100006 suid=100006 fsuid=100006 egid=100001 sgid=100001 fsgid=100001 tty=(none)
ses=4294967295 comm="keysafe5-agent" exe="/opt/nfast/sbin/keysafe5-agent" subj=keysafe5-agent key=(null)
Dec 10 19:04:32 nshield-64DB-8D35-0405 keysafe5-agent[158675]: enabled journal logging
Dec 10 19:04:32 nshield-64DB-8D35-0405 keysafe5-agent[158675]: Updated agent config: Hostname:hsm_64DB-
8D35-0405, Version:1.5.0-e4687903, MessageBus:{URL: tls://10.194.148.22:18084, tls: true},
LoggerConfig:{level:Info, format:JSON, file.enabled:false, file.path:/opt/nfast/log/keysafe5-agent.log,
journal.enabled: true}, UpdateInterval:1m0s, HealthInterval:1m0s, RecoveryInterval:5s,
KmdataNetworkMount:false, KmdataPollInterval:1s, CodeSafeUpdateInterval:3m0s, CodeSafeCachePeriod:1h0m0s
Dec 10 19:04:32 nshield-64DB-8D35-0405 keysafe5-agent[158675]: Starting agent
```

2. If the agent logs indicate message bus connection errors like the following, stop and restart the KeySafe 5 server using the steps below.

```
An example of message bus connectivity errors:

Dec 10 19:04:38 nshield-64DB-8D35-0405 keysafe5-agent[158675]: Error starting agent: message bus connection
error: failed to create NATS connection for publishing: nats: no servers available for connection
```

   How to restart a Linux KeySafe 5 server:

```
/opt/nfast/scripts/init.d/keysafe5-server stop
/opt/nfast/scripts/init.d/keysafe5-server start
```

   How to restart a Windows KeySafe 5 server:

   a. Launch the **Services** window.
   b. Right-click **nShield KeySafe 5**, then select **Stop** and **Start**.

Chapter 5. Additional resources and related products