



HID Global Validation Authority

nShield® HSM Integration Guide

2025-07-18

Table of Contents

1. Introduction	1
1.1. Product configurations	1
1.2. Supported nShield hardware and software versions	1
1.3. Supported nShield HSM functionality	1
1.4. Requirements	2
1.5. More information	3
2. Procedures	4
2.1. Install Java	4
2.2. Install the HSM	4
2.3. Install the Security World software and create a Security World	4
2.4. Create the OCS	6
2.5. Configure Java	6
2.6. Install and configure the database	6
2.7. Install the HID Global Validation Authority	9
2.8. Configure the HID Global Validation Authority	10
2.9. Start the HID Global Validation Authority	14
3. Additional resources and related products	16
3.1. nShield Connect	16
3.2. nShield as a Service	16
3.3. Entrust products	16
3.4. nShield product documentation	16

Chapter 1. Introduction

The nShield Hardware Security Module (HSM) can generate and store a Root of Trust that protects security objects used by HID Global Validation Authority to safeguard user keys and credentials. You can use the HSM in FIPS 140 Level 2 or Level 3 mode to meet compliance requirements.

1.1. Product configurations

Entrust has tested nShield HSM integration with HID Validation Authority in the following configurations:

Product	Version
Operating System	Windows Server 2022
HID ActivID VA	7.4
Database	Microsoft SQL Server 2025
Java	jdk-11 or higher (windows-x64)

1.2. Supported nShield hardware and software versions

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

Product	Security World Software	Firmware	Image
Connect XC	13.6.11	12.72.1 (FIPS 140-2 certified)	13.6.7
nShield 5c	13.6.11	13.4.5 (FIPS 140-3 certified)	13.6.7

1.3. Supported nShield HSM functionality

Feature	Support
Module-only key	No
OCS cards	Yes
Softcards	No

Feature	Support
nSaaS	Yes
FIPS 140 Level 3	Yes

1.4. Requirements

Before installing these products, read the associated documentation:

- For the HSM: *Installation Guide* and *User Guide*.
- For Remote Administration (if used): *nShield Remote Administration User Guide*.
- HID Global documentation: *ActivID® Validation Authority Installation and Configuration Guide*.

The integration between nShield HSMs and HID VA requires:

- nCipherKM JCA/JCE CSP support in the HSM.
- A correct quorum for the Administrator Card Set (ACS).
- An Operator Card Set (OCS).
 - A 1-of-N quorum must be used.
- Firewall configuration with usable ports:
 - 9004 for the HSM (hardserver).
 - 3501 for HID VA HTTP Port (default port number).
 - 3601 for HID VA HTTPS Port (default port number).

In addition, the following design decisions have an impact on how the HSM is installed and configured:

- Whether your Security World must comply with FIPS 140 Level 3 standards.

If you are using FIPS 140 Level 3, it is advisable to create an OCS for FIPS authorization. It will be needed during the Validation Authority Configuration. For information about limitations on FIPS authorization, see the *Installation Guide* for the HSM.

- Whether to instantiate the Security World as recoverable or not.



Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

1.5. More information

For more information about OS support, contact your HID Global sales representative or Entrust nShield Support, <https://nshieldsupport.entrust.com>.



Access to the Entrust Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

Chapter 2. Procedures

2.1. Install Java

1. Install the Java Development Kit (JDK).



HID specifically requires the JDK and not the Java Runtime Environment (JRE). Refer to the HID documentation for validated versions of the JDK.

2. Set the **JAVA_HOME** environment variables

```
>export JAVA_HOME=/usr/lib/jvm/java-11-openjdk
>export JRE_HOME=/usr/lib/jvm/java-11-openjdk
>export PATH=$JAVA_HOME/bin:$PATH
```

2.2. Install the HSM

Install the nShield Connect HSM locally, remotely, or remotely via the serial console. See the following nShield Support articles and the *Installation Guide* for the HSM:

- [How to locally set up a new or replacement nShield Connect](#)
- [How to remotely set up a new or replacement nShield Connect](#)
- [How to remotely set up a new or replacement nShield Connect XC Serial Console model](#)



Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

2.3. Install the Security World software and create a Security World

1. Install the Security World software:
 - a. Mount the DVD or .iso/disc image and locate **setup.exe**.
 - b. Right-click the **setup.exe** icon and select **Run as Administrator**.
 - c. For detailed instructions, see the *Installation Guide* and the *User Guide* for the HSM.
2. Add the Security World utilities path **C:\Program Files\nCipher\ncfast\bin** to the

Windows system path.

3. Open the firewall port 9004 for the HSM connections.
4. Enroll the HSM:

```
>nethsmenroll -m 1 -f -p 10.194.148.30
Remote module returned ESN: 6308-03E0-D947
HKNETI: 5b8a765a49d46d2c186aec5b189387cb9716573e
Is the above correct? (yes/no): yes
OK configuring hardserver's nethsm imports
```

5. Open a command window and run the following command to confirm that the HSM is **operational**:

```
>enquiry
Server:
  enquiry reply flags  none
  enquiry reply level Six
  serial number       6308-03E0-D947
  mode                 operational
...
Module #1:
  enquiry reply flags  none
  enquiry reply level Six
  serial number       6308-03E0-D947
  mode                 operational
...
```

6. Create your Security World if one does not already exist, or copy an existing one.
Follow your organization's security policy for this.
7. Confirm that the Security World is **usable**:

```
>nfkminfo
World
  generation 2
  state      0x3fb7000c Initialised Usable ...
...
  mode      fips1402level3

Module #1
  generation 2
  state      0x2 Usable
```

8. Edit the **C:\ProgramData\nCipher\Key Management Data\config\config** file. Add the following lines in the **[server_startup]** section:

```
[server_startup]
...
priv_port=9001
nonpriv_port=9000
```

2.4. Create the OCS

To create the OCS

1. Create the OCS, following your organization's security policy for the value N of K/N. As required, create extra OCS cards, one for each person with access privilege, plus spares.



Administrator Card Set (ACS) authorization is required to create an OCS in FIPS 140 level 3.



After an OCS card set has been created, the cards cannot be duplicated.

```
# createocs -m1 -s2 -N HIDValAuth -Q 1/1

FIPS 140-2 level 3 auth obtained.

Creating Cardset:
Module 1: 0 cards of 1 written
Module 1 slot 3: Admin Card #1
Module 1 slot 2: blank card
Module 1 slot 0: empty
Module 1 slot 2:- passphrase specified - writing card
Card writing complete.

cardset created; hkltu = 6165632fe011c6475f4d61ac555698d437230cf3
```

2. List the OCS created:

```
>nfkminfo -c
Cardset list - 1 cardsets: (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
Operator logical token hash          k/n timeout name
6165632fe011c6475f4d61ac555698d437230cf3  1/1  none-NL  HIDValAuth
```

2.5. Configure Java

To configure Java:

1. Copy the `nCipherKM.jar` file from `%NFAST_HOME%\java\classes\` to the extensions folder of the local Java `%JAVA_HOME%\lib`:

```
>copy "C:\Program Files\nCipher\nfast\java\classes\nCipherKM.jar" "C:\Program Files\Java\jdk-11.0.22\jre\lib\."
1 file(s) copied.
```

2.6. Install and configure the database

To install and configure the database:

1. Install the database where information about issuers, credentials, and revocation lists will be stored. See the HID documentation for compatible database versions.
2. Create a new database called **rtc**.
3. Create a new login as follows:
 - a. For **Login name**, enter **rtc**.
 - b. Select **SQL server authentication**.
 - c. Enter a **Password** and confirm the password.
 - d. For **Default database**, select **rtc**. For example:

Script Help

Login name: Search...

☐ Windows authentication

☒ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy

☒ Enforce password expiration

☒ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential

Add

Credential	Provider
------------	----------

Remove

Default database:

Default language:

- e. For **Users mapped to this login**, select **rtc**.
- f. For **Access privilege**, select **db_datareader**, **db_datawriter**, **db_ddladmin**, **db_owner**, and **public**. For example:

Script Help

Users mapped to this login:

Map	Database	User	Default Schema
<input type="checkbox"/>	master		
<input type="checkbox"/>	model		
<input checked="" type="checkbox"/>	rtc	rtc	
<input type="checkbox"/>	tempdb		

☐ Guest account enabled for: rtc

Database role membership for: rtc

<input type="checkbox"/>	db_accessadmin
<input type="checkbox"/>	db_backupoperator
<input checked="" type="checkbox"/>	db_datareader
<input checked="" type="checkbox"/>	db_datawriter
<input checked="" type="checkbox"/>	db_ddladmin
<input type="checkbox"/>	db_denydatareader
<input type="checkbox"/>	db_denydatawriter
<input checked="" type="checkbox"/>	db_owner
<input type="checkbox"/>	db_securityadmin
<input checked="" type="checkbox"/>	public

- g. For **Server authentication**, select **SQL Server and Windows Authentication mode**.

Script Help

Server authentication

☐ Windows Authentication mode

☒ SQL Server and Windows Authentication mode

Login auditing

☐ None

☒ Failed logins only

☐ Successful logins only

☐ Both failed and successful logins

Server proxy account

☐ Enable server proxy account

Proxy account:

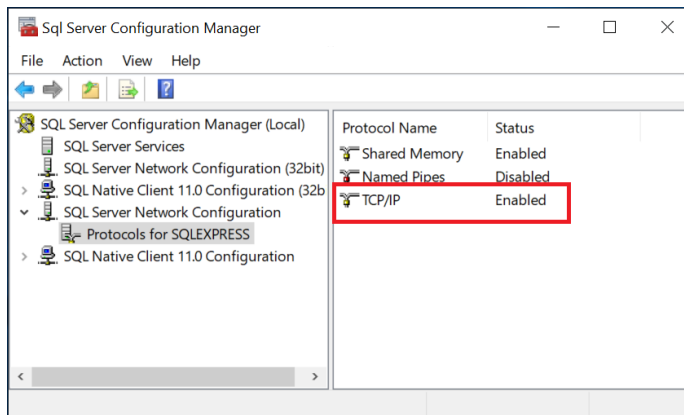
Password:

Options

☐ Enable C2 audit tracing

☐ Cross database ownership chaining

4. Enable the TCP/IP network protocol.

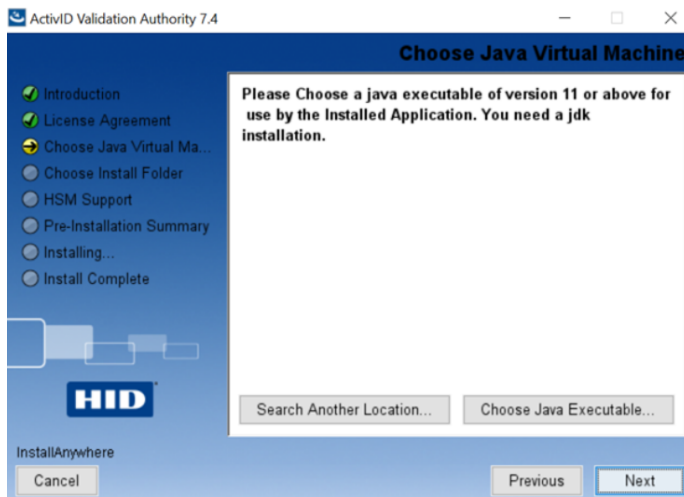


5. Open the firewall port 1433 for the TCP/IP connection to the MS SQL server.

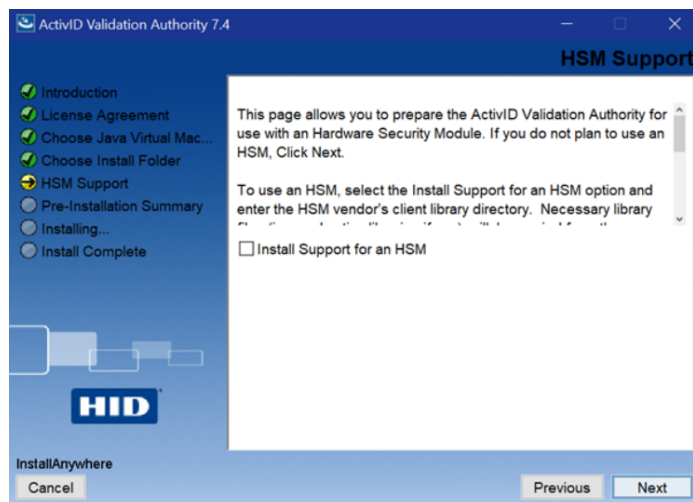
2.7. Install the HID Global Validation Authority

For detailed instructions, see the *ActiviD® Validation Authority Installation and Configuration Guide*.

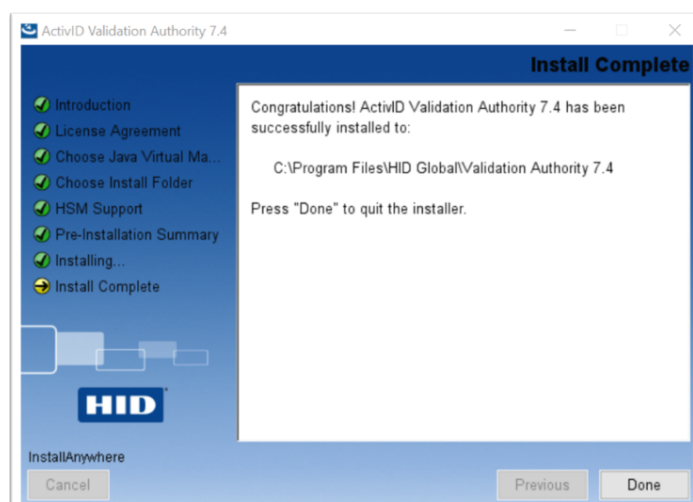
1. Run through the HID VA installer.
2. On the **Choose Java Virtual Machine** page of the installer, choose the Java executable within the JDK folder.



3. On the **HSM Support** page of the installer:
 - a. Select **Install Support for an HSM**.
 - b. Select **Choose** and find `%NFAST_HOME%\java\classes`.



4. Complete the installation.



5. Launch the Windows Services and locate **ActivID Validation Authority**.
6. Right-click **ActivID Validation Authority** to select its properties.
7. On the **General** tab, for **Startup type** select **Manual**.
8. On the **Log On** tab, select **Local System account**.
9. Select **Apply** and then select **OK**.

2.8. Configure the HID Global Validation Authority

1. Insert the OCS in the HSM.
2. On the Windows **Start** menu, run **Configure Validation Authority**.
3. Select **Begin**.
4. Select whether you are upgrading or new installation.
5. On the next page, provide your organization name.

6. On the **Keystore** page:

- a. Select **nShield (client software v11 or later)** from the drop-down menu.
- b. Clear the **Oracle SunJCE keystore for SSL Key** check box.
- c. Select **Regenerate Keys** to create a new set of security keys that are protected by the nShield HSM.
- d. Select all four key options if this is a fresh install.



This version of the VA has a known issue. It does not support an ECC key for the **Asymmetric SSL Key** option. If you want to install the VA using ECC keys, contact HID for more information.

e. Under **Message Digest Algorithms**:

- i. For the **For Signatures** property, select **SHA-256**.
- ii. For the **For OCSP Response Data** property, select **SHA-256**.

f. Under **Keystore Password (Required)**

- i. Select **Prompt for Password at Server Start**.
- ii. Enter and confirm the enter the OCS passphrase.

g. Select **Next**.

7. In the **Configure Database** page:

- a. For **Vendor**, select **Microsoft SQL Server**.
- b. For **Host**, enter **localhost**.
- c. For **Port**, enter **1433**.
- d. For **Database**, enter **rtc**.
- e. For **User**, enter **rtc**.
- f. For **Password**, enter the database password defined in [Install and configure the database](#).
- g. Select **Next**.

The screenshot shows the 'Configure Database' section of the HID ActivID Validation Authority Configuration tool. On the left is a sidebar with a list of steps: Welcome, Upgrade, Organization Name, Keystore, Database (selected), Multi-Person Control, Admin Account, Proxy, Ports and Ciphers, Start/Restart Server, and Complete. The main content area is titled 'Configure Database' and includes a description: 'The ActivID Validation Authority stores information about issuers, credentials, and revocation lists in a standard SQL database. This requires several configuration parameters to determine where the database is located and how the ActivID Validation Authority will log into the database.' Below this is a form with the following fields: Vendor (Microsoft SQL Server), Host (localhost), Port (1433), Database (rtc), Username (rtc), and Password (masked with dots). At the bottom of the form are three buttons: 'Previous', 'Next', and 'Quit Configuration'.

8. In the **Initialize Database** page:

- Clear the **Remove all ActivID Validation Authority data and drop tables** check box.
- Select **Create required tables**.
- Select **Next**.

The screenshot shows the 'Initialize Database' section of the HID ActivID Validation Authority Configuration tool. The sidebar on the left is the same as in the previous screenshot, with 'Database' selected. The main content area is titled 'Initialize Database' and includes a description: 'There are several tables required for the ActivID Validation Authority to function. If you are configuring a new Authority installation, you must check "Create...". If you are reconfiguring an existing Authority installation and want to re-initialize the database, you should check both "Remove..." and "Create...". NOTE: This will erase all existing ActivID Validation Authority data permanently. If you are reconfiguring an existing Authority installation and want to retain your existing ActivID Validation Authority information, leave both boxes unchecked.' Below this is a form with two checkboxes: 'Remove all ActivID Validation Authority data and drop tables' (unchecked) and 'Create required tables' (checked). At the bottom of the form are three buttons: 'Previous', 'Next', and 'Quit Configuration'.

9. In the **Multi-Person Control** page, select **Next**.

The screenshot shows the 'Multi-Person Control' section of the HID ActivID Validation Authority Configuration tool. The sidebar on the left is the same as in the previous screenshots, with 'Multi-Person Control' selected. The main content area is titled 'Multi-Person Control' and includes a description: 'The ActivID Validation Authority can be configured to require the approval of multiple users when adding new Certificate Issuers or user Accounts to the system. This level of security is typically only needed for Delegated Path Validation operations and should not be enabled without reading and understanding the appropriate sections of the product documentation. There are not currently enough user accounts to allow multi-person control to be used. If you wish to enable multi-person control, check the box below, then use the ActivID Validation Authority Management Console to configure and cross-sponsor all of the user accounts that will be needed. Once you have created and cross-sponsored all of the user accounts, rerun this tool and set the desired number of required sponsors.' Below this is a form with a checkbox labeled 'Multi-Person Control Required:' which is unchecked. At the bottom of the form are three buttons: 'Previous', 'Next', and 'Quit Configuration'.

10. In the **Administrator Account** page:

- Enter the credentials for the HID Global Validation Authority.
- Select **Next**.

The screenshot shows the 'Administrator Account' section of the HID ActivID Validation Authority Configuration tool. The sidebar on the left is the same as in the previous screenshots, with 'Admin Account' selected. The main content area is titled 'Administrator Account' and includes a description: 'No administrator account was found in the ActivID Validation Authority database. To create an administrator account, enter the information below.' Below this is a form with three fields: 'Login' (admin), 'Password' (masked with dots), and 'Confirm' (masked with dots). At the bottom of the form are three buttons: 'Previous', 'Next', and 'Quit Configuration'.

11. In the **Proxy** page, do not update any properties. Then, select **Next**.

ActivID Validation Authority Configuration

Welcome

Upgrade

Organization Name

Keystore

Database

Multi-Person Control

Admin Account

Proxy

Pois and Ciphers

Start/Restart Server

Complete

Proxy

The ActivID Validation Authority can access HTTP resources through a proxy server. If your network uses a proxy server for HTTP traffic, use this page to configure the Authority to use it.
If your network does not use a proxy leave the "Proxy Server" field blank.

Proxy Server:

Port:

☐ Authentication Required

User Name:

Password:

PreviousNext


Quit Configuration

12. In the **Ports** page, do not update any properties. Then, select **Next**.

[illegible]

13. Select **Start/Restart** to finish.

- [Welcome](#)
- [Upgrade](#)
- [Organization Name](#)
- [Keystore](#)
- [Database](#)



Start/Restart Authority

The changes made to the ActivId Validation Authority configuration will not take effect until the Authority is started (or restarted if it is already running). To start or restart the Authority, click the "Start/Restart" button below. If you plan to start or restart the Authority manually, click "Next."


Previous
Start/Restart
Next

Quit Configuration

A password dialog appears. Be aware that the dialog may be behind the Browser window.

14. Enter the OCS passphrase and select **OK**.

The installation completes.



ActivID Validation Authority
Configuration

Configuration Complete

Configuration of the ActivID Validation Authority is now complete and the configuration server has been stopped. Continue on to the [Management Console](#) to administer the ActivID Validation Authority or close this browser window to quit configuration.

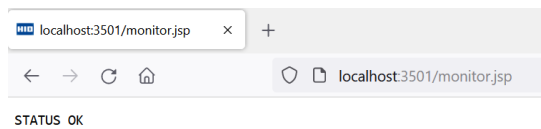
- Welcome
- Upgrade
- Organization Name
- Keyspace

Configuration Complete

Configuration of the ActivID Validation Authority is now complete and the configuration server has been stopped. Continue on to the [Management Console](#) to administer the ActivID Validation Authority or close this browser window to quit configuration.

15. Verify the installation:

- a. Close your browser.
- b. Open your browser and enter the following URL
http://localhost:3501/monitor.jsp.



- c. Confirm that **STATUS OK** appears.

2.9. Start the HID Global Validation Authority

To start the HID Global Validation Authority:

1. Insert the OCS card into the HSM.
2. Open a command prompt and start HID VA.

```
C:\Program Files\HID Global\Validation Authority 7.4\authority\bin>server.bat start
Using CATALINA_BASE:  "C:\Program Files\HID Global\Validation Authority 7.4\authority"
Using CATALINA_HOME:  "C:\Program Files\HID Global\Validation Authority 7.4\authority\..\tomcat"
Using CATALINA_TMPDIR: "C:\Program Files\HID Global\Validation Authority 7.4\authority\temp"
Using JRE_HOME:       "C:\Program Files\Java\jdk-11.0.22"
Using CLASSPATH:      "C:\Program Files\HID Global\Validation Authority
7.4\authority\..\tomcat\bin\bootstrap.jar;C:\Program Files\HID Global\Validation Authority
7.3\authority\..\tomcat\bin\tomcat-juli.jar"
Using Security Manager
```



Entrust was unable to start the HID VA service from services as detailed in the HID Global documentation. The **server.bat** file was used instead.

A password dialog appears. Be aware that the dialog may be behind the Browser window.

3. Enter the OCS passphrase.
4. Access the HID Validation Authority Management Console from a web browser. To do this, select **Start > HID Global > Validation Authority Management**.

https://localhost:3601/va/login.jsp

HID

ActivID Validation Authority
Management Console

Login: admin

Password: ●●●●●●●●

Login

Chapter 3. Additional resources and related products

3.1. nShield Connect

3.2. nShield as a Service

3.3. Entrust products

3.4. nShield product documentation