

HID Global Validation Authority

nShield® HSM Integration Guide

2026-11-2

© Entrust Corporation. All rights reserved.

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 . . . 2
    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. Create the OCS . . . 5
    2.4. Configure Java for nShield . . . 6
    2.5. Install Microsoft SQL Server . . . 6
    2.6. Configure the HID VA database . . . 7
    2.7. Install the HID Global Validation Authority . . . 9
    2.8. Configure the HID Global Validation Authority . . . 11
    2.9. Start the HID Global Validation Authority . . . 14
    2.10. Optional OCSP test . . . 15
3. Additional resources and related products . . . 17
    3.1. nShield HSMs . . . 17
    3.2. nShield as a Service . . . 17
    3.3. Entrust products . . . 17
    3.4. nShield product documentation . . . 17

Chapter 1. Introduction

The nShield Hardware Security Module (HSM) serves as a root of trust for the cryptographic material used by the HID Global Validation Authority. Integrating HID Global Validation Authority with an Entrust nShield HSM helps meet strict compliance requirements by providing FIPS 140-3 or FIPS 140-2 protection.

1.1. Product configurations

This integration guide is intended solely to demonstrate the integration process and does not represent best practices. For guidance on optimal implementation, consult your organization's IT security team or engage Entrust Professional Services.

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

HID ActivID VA	Operating System	Database	Java
7.5	Windows Server 2025	Microsoft SQL Server 2025, 2019	Microsoft Build of OpenJDK 17.0.12
7.4	Windows Server 2022	Microsoft SQL Server 2022	JDK-11 or higher (windows-x64)
7.3	Windows Server 2019	Microsoft SQL Server 2019	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 13.6.18	12.72.1, 12.72.3 and 12.72.4 (FIPS 140-2 certified)	13.6.7 13.6.18
nShield 5c	13.6.11 13.6.18	13.4.5 (FIPS 140-3 certified)	13.6.7 13.6.18

1.3. Supported nShield HSM functionality

Feature	Support
Module-only key	No
Softcards	No
OCS cards	Yes
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* at the nShield user documentation site.
- For Remote Administration (if used): *nShield Remote Administration User Guide* at the nShield user documentation site.
- HID Global documentation: *ActivID® Validation Authority Installation and Configuration Guide* at the HID documentation portal.



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

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 that allows traffic on the following ports:
  - 9004 for the HSM (hardserver).
  - 3501 for the HID VA HTTP port (default).
  - 3601 for the HID VA HTTPS port (default).

In addition, the following design decisions affect how the HSM is installed and configured:

- Whether your Security World must comply with FIPS 140-3 or 140-2 standards.

If you are using FIPS 140-3 or 140-2, creating an OCS for FIPS authorization is advisable. The OCS is needed during 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.

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

HID Global Validation Authority requires a Java Development Kit (JDK), not a Java Runtime Environment (JRE). For VA 7.5, HID lists the Microsoft Build of OpenJDK 17.0.12 as a supported version.

1. Download and install the Microsoft Build of OpenJDK for all users.
   In the installer, enable **Modify PATH variable** and **Set or override JAVA_HOME variable**.
2. Open a new PowerShell window and verify that the JDK is available:

   ```
   java -version
   javac -version
   $env:JAVA_HOME
   ```

   Confirm `java` and `javac` report the expected JDK version.

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 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.

1. Install the Security World software on the Windows server running HID VA.

   Ensure the client components are installed and that the Security World utilities are available in the system `PATH`. Restart the server after installation.

   Refer to the nShield Security World documentation for more information.

2. Use your organization's approved HSM administration workflow to register the Windows server running HID VA as an HSM client.

3. In an elevated PowerShell window on the HID VA server, enroll the client with each HSM:

```
nethsmenroll <HSM-IP-address>
```

4. Confirm that the HSM is operational by running `enquiry`.

   For a high-availability setup, confirm that each HSM is listed and operational. Confirm that the server can reach each HSM over TCP port `9004` before continuing.

5. Load an approved existing Security World or create one according to your organization's Security World policy.

   Do not copy Security World files from an unverified source.

6. Run `nfkminfo` and confirm that the World state and the target module state are both `usable`.
7. Run `nfkmcheck` and confirm that it reports `everything seems to be in order` before continuing.
8. Configure the client ports in `C:\ProgramData\nCipher\Key Management Data\config\config`:

   In the `[server_startup]` section, set the following values, verifying and editing existing settings rather than adding duplicates:

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

9. If you changed the port values, restart the hardserver. The new ports take effect when the hardserver next starts.
10. If cardlist allowlisting is enabled, authorize the OCS card or cards required by HID VA using your organization's card-management policy.

    Do not use a wildcard allowlist entry in a customer environment.

See Configuring the nShield HSM to use the client and Configuring client computers to use the nShield HSM for details.

2.3. Create the OCS

1. Create the OCS with a 1-of-N quorum. Choose N in accordance with your organization's security policy.

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 <OCS-name> -Q <K>/<N>
```

2. Confirm the OCS is listed with the expected name and quorum:

```
nfkminfo -c
```

2.4. Configure Java for nShield

Copy the nShield Java provider into the library directory of the selected JDK:

```
Copy-Item "$env:ProgramFiles\nCipher\nfast\java\classes\nCipherKM.jar" "$env:JAVA_HOME\lib\"
```

2.5. Install Microsoft SQL Server

HID VA 7.5 documentation lists SQL Server 2019 Express, Standard, and Enterprise editions. SQL Server 2025 has also been tested successfully, but HID does not list it as an officially supported version. Use approved installation media; setup screens and options may vary by SQL Server release.

1. Run `setup.exe` as Administrator and select a new stand-alone SQL Server installation.
2. Install **Database Engine Services**. Use the default instance when available. If you use a named instance, record its name for later configuration.
3. For the **Database Engine Configuration**, select **Mixed Mode**.
4. Add the Windows account that will create the HID VA database as a SQL Server administrator and set a strong administrator password in accordance with your organization's policy.
5. In SQL Server Configuration Manager, enable TCP/IP for the instance:
   - Set **IPAll** to a fixed TCP port, `1433`.
   - Clear **TCP Dynamic Ports**.
   - Restart the SQL Server instance.
6. Verify that SQL Server is listening on port `1433` and that `Test-NetConnection -ComputerName localhost -Port 1433` succeeds before configuring HID VA.

When SQL Server and HID VA are on the same machine, do not add an inbound firewall rule

for port 1433. For a separate database server, use its hostname and restrict inbound TCP 1433 to the HID VA server's address.

2.6. Configure the HID VA database

1. Create a database named `rtc` to store HID VA issuer, credential, and revocation-list data. Do not create the VA tables manually; the HID configuration wizard creates them.
2. Create a new login:

    a. For **Login name**, enter `rtc`.

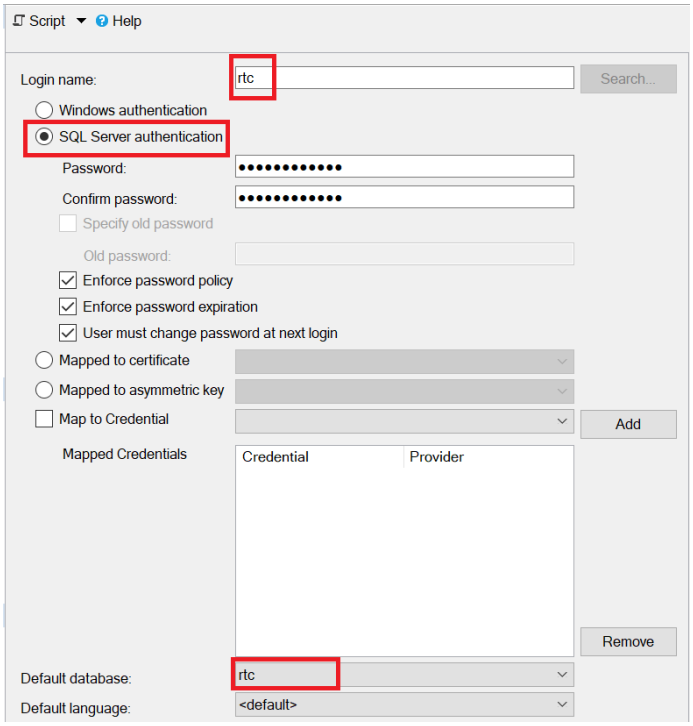
    b. Select **SQL server authentication**.

    c. Enter and confirm a **Password**.

    d. For **Default database**, select **rtc**.

    e. Enable password policy and expiration in accordance with your organization's account policy.

    For example:

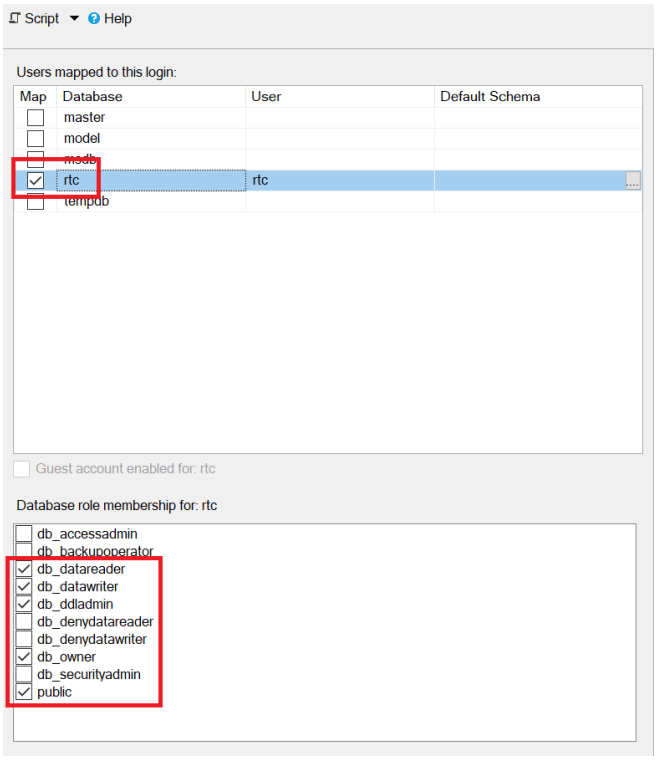


    a. For **Users mapped to this login**, select **rtc**.

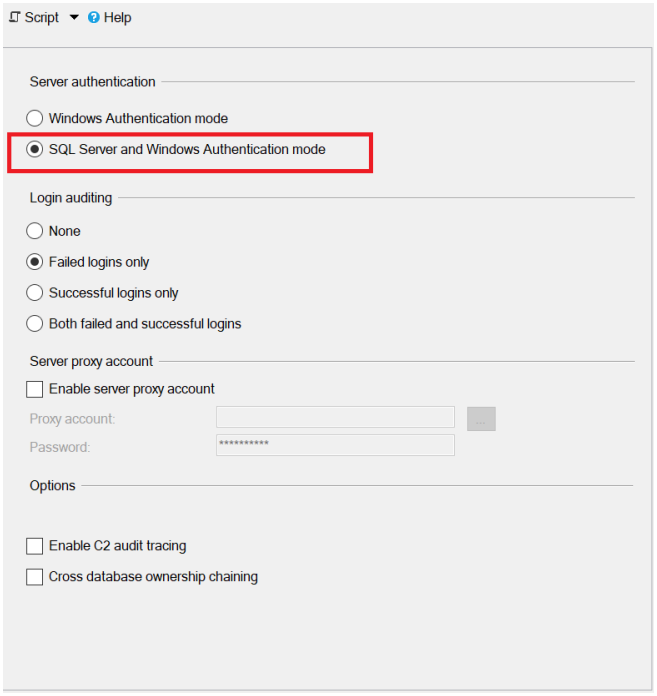
    b. For **Access privilege**, select **db_datareader**, **db_datawriter**, **db_ddladmin**, and **db_owner**.

    Membership in **public** is automatic; do not grant the login server-level sysadmin access for the application.

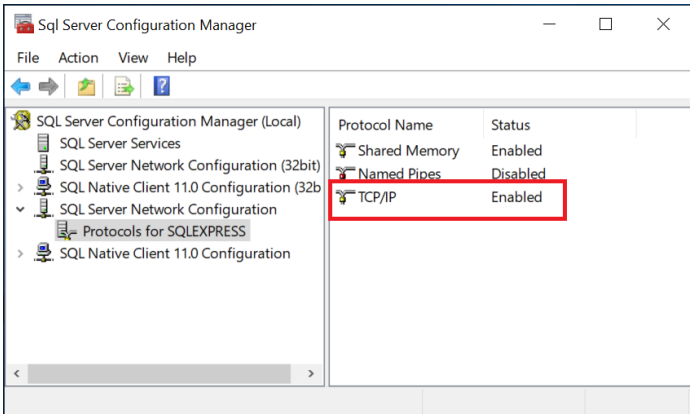
For example:



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



3. Enable the TCP/IP network protocol.



4. Verify that Mixed Mode authentication is enabled and that the SQL Server instance is listening on TCP port `1433`. Do not open inbound port `1433` when SQL Server and HID VA run on the same machine.
5. Verify the `rtc` login using `sqlcmd`.

   Because `-P` is omitted, the command prompts for the SQL password instead of placing it on the command line:

   ```
   sqlcmd -S tcp:localhost,1433 -U rtc -C -b -Q "SELECT ORIGINAL_LOGIN() AS LoginName, DB_NAME() AS
   DatabaseName; SELECT IS_MEMBER('db_owner') AS IsDatabaseOwner;"
   ```

   Confirm the following details:

   - `LoginName` is `rtc`
   - `DatabaseName` is `rtc`
   - `IsDatabaseOwner` is `1`

   Do not use the `sa` account for the HID VA database connection.

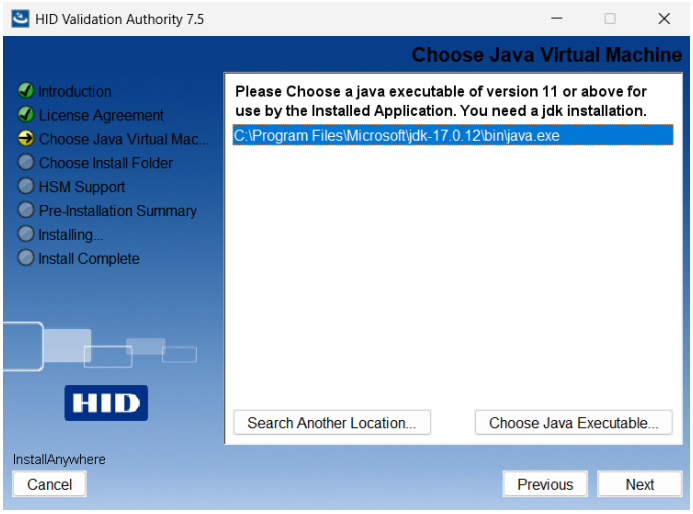
2.7. Install the HID Global Validation Authority

The following steps describe how to install HID VA 7.5 on Windows. For other releases, use the matching *ActivID® Validation Authority Installation and Configuration Guide* and installer package.

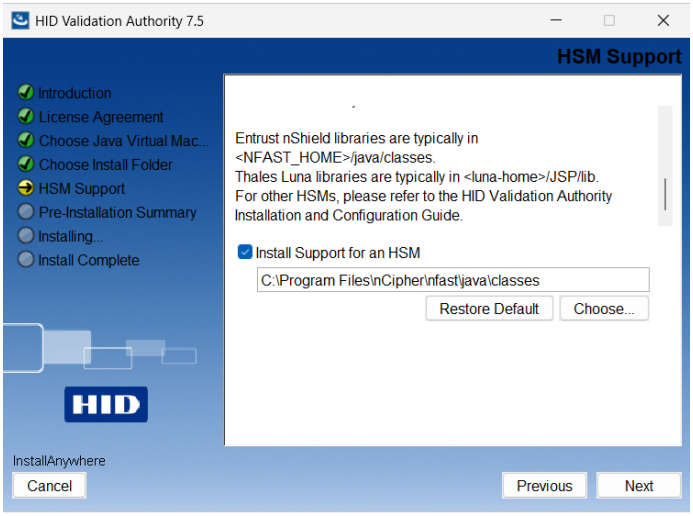
1. From the HID customer portal, download the full HID Validation Authority 7.5 software ZIP.
2. Extract the ZIP to a local staging folder; do not run the installer from inside the archive.
3. Locate the installer in the extracted `Products` folder and confirm that the nShield Java provider is installed.
   If VA is already installed, exit the installer on its first page. Do not select a repair,

removal, or installation option.

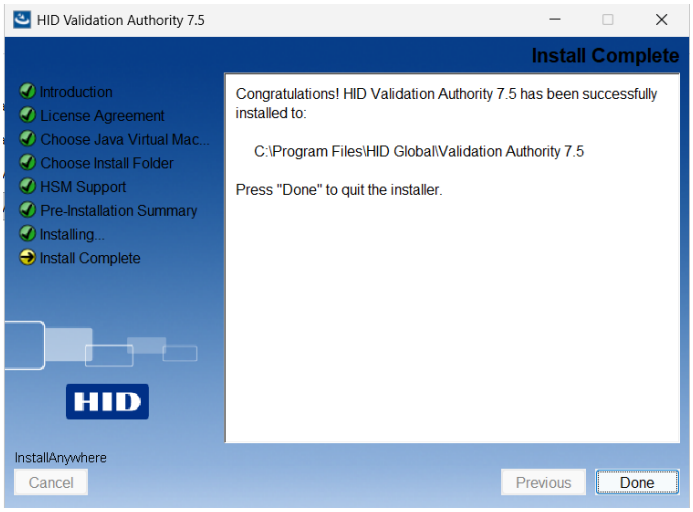
4. Run the installer from the extracted `Products` folder, using the JDK selected for HID VA.
5. On the **Choose Java Virtual Machine** page of the installer, choose the Java executable within the JDK folder.



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



7. Complete the installation.



8. Open Windows Services and locate **ActivID Validation Authority**.
9. Right-click **ActivID Validation Authority** and select **Properties**.
10. On the **General** tab, set **Startup type** to **Manual**.
11. On the **Log On** tab, select **Local System account**.
12. Select **Apply** and then select **OK**.

You must configure the keys, database connection, tables, and administrator account before starting the VA server.

2.7.1. Apply the VA cumulative hotfix

If a cumulative hotfix is available for this VA release, download the hotfix and its README from the HID portal. Hotfixes are cumulative, so apply only the latest hotfix available for this release.



Because the hotfix cannot be uninstalled, create a backup or VM snapshot before applying it.

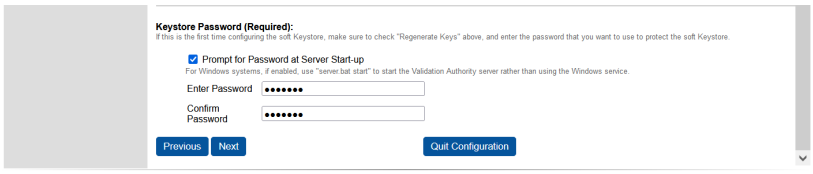
Stop the HID Validation Authority service and follow the matching vendor instructions before proceeding. Leave SQL Server and nShield services running unless the hotfix instructions state otherwise.

2.8. Configure the HID Global Validation Authority

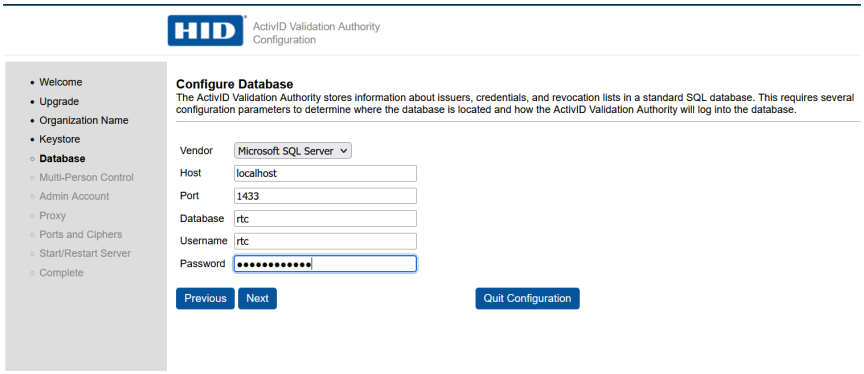
1. Make the OCS card available in the HSM's physical reader or slot 0.
2. From the Windows **Start** menu, run **Configure Validation Authority** and select **Begin**.
3. Indicate whether this is an upgrade or a new installation.

If it is an upgrade, follow the version-specific HID upgrade guidance before continuing.

4. On the next page, provide your organization name.
5. On the **Keystore** page:
    a. Select **Entrust nShield (client software v11 and 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.
    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 OCS passphrase.



    g. Select **Next**.
6. On the **Configure Database** page:
    a. For **Vendor**, select **Microsoft SQL Server**.
    b. For **Host**, enter **localhost** or the database server hostname, as applicable.
    c. For **Port**, enter **1433**.
    d. For **Database**, enter **rtc**.
    e. For **User**, enter **rtc**.
    f. For **Password**, enter the `rtc` SQL login password defined in Configure the HID VA database. Do not use the SQL Server `sa` account for the application connection.
    g. Select **Next**.

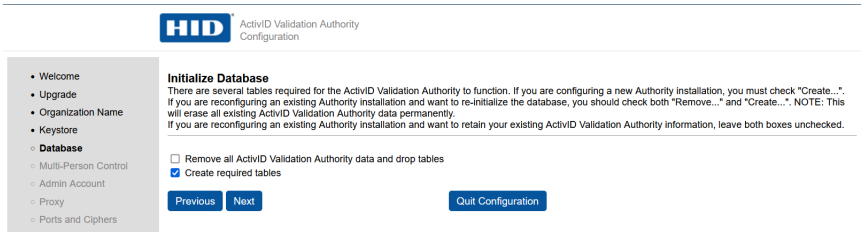


7. In the **Initialize Database** page:

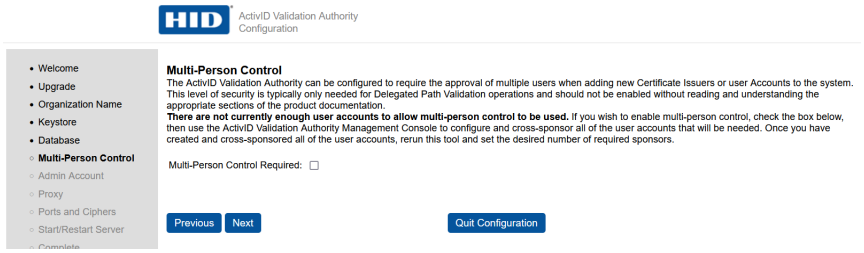
   a. Clear the **Remove all HID Validation Authority data and drop tables** check box.

   b. Select **Create required tables**.

   c. Select **Next**.



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

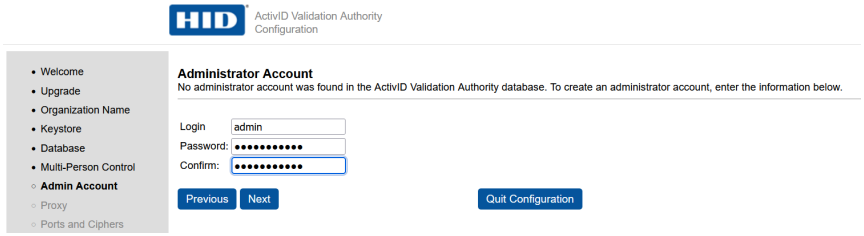


9. In the **Administrator Account** page:

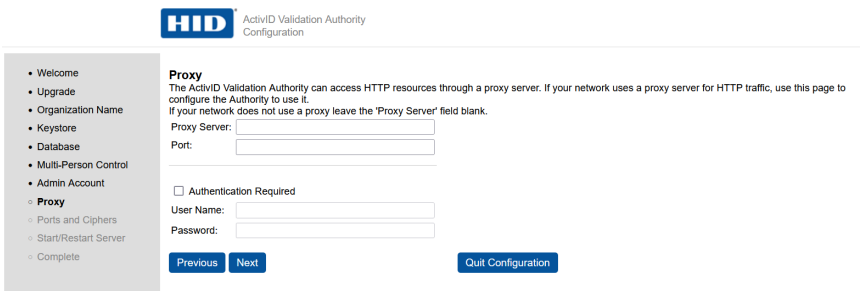
   a. Enter the credentials for the HID Global Validation Authority.

   b. Create the HID VA administrator account according to your organization's account and password policies.

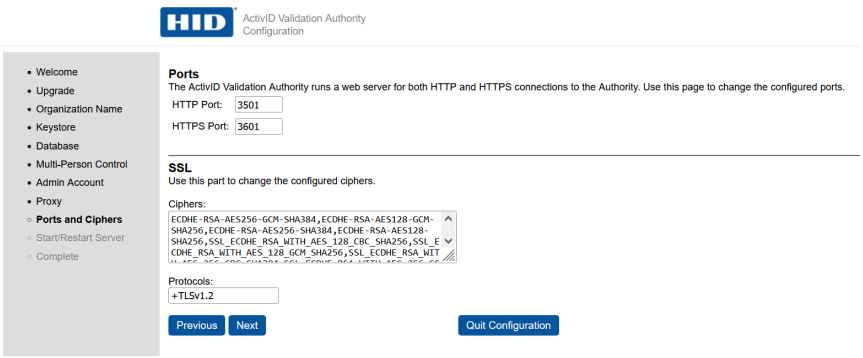
   c. Select **Next**.



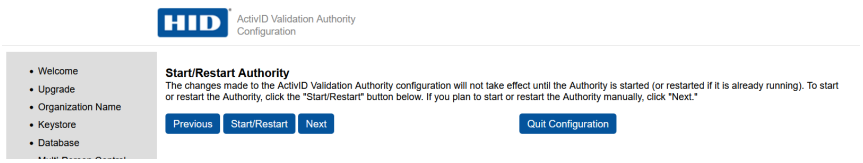
10. On the **Proxy** page, keep the defaults unless your environment requires a proxy, then select **Next**.



11. On the **Ports** page, keep the defaults unless your deployment requires different ports, then select **Next**.



12. On the **Start/Restart Authority** page, select **Next** to finish configuration without starting the service.



Close the browser when configuration is complete.

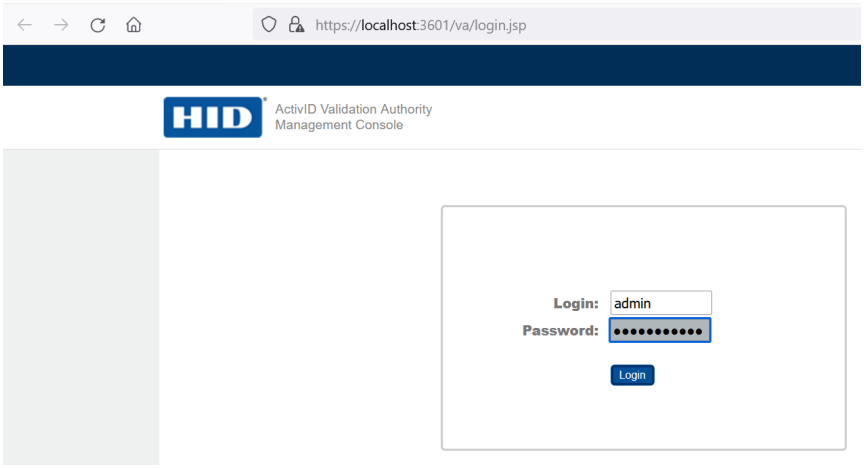
2.9. Start the HID Global Validation Authority

1. Place the OCS card in the HSM's physical reader or in slot 0.
2. Open a command prompt in the installed VA `authority\bin` directory and start the server:

```
server.bat start
```

3. Enter the OCS passphrase when prompted, and keep the Tomcat terminal open.

4. Open `http://localhost:3501/monitor.jsp` and confirm that **STATUS OK** appears.
5. Open the HID Validation Authority Management Console from the Windows **Start** menu by selecting **HID Global** > **Validation Authority Management**.



Alternatively, open `http://localhost:3501/va/login.jsp` and sign in with the administrator account created during configuration.

2.10. Optional OCSP test

Use an existing revoked certificate to verify that HID VA reads the issuing CA's current base CRL and returns a signed OCSP response. HID VA acts as the responder; a separate OCSP service is not required.

Before testing:

- Make sure that the following items are available on the server:
  - The issuing CA certificate
  - The issuing CA certificate's current base CRL
  - The VA OCSP signing certificate available on the VA server.
- Confirm that the issuing CA and base CRL are registered in HID VA.
- Use PEM-encoded certificate files named `issuer-ca.pem` and `va-ocsp-signing.pem`, and the CRL file `issuer-ca.crl` in the working directory.
- If the certificates are DER-encoded, convert them to PEM with OpenSSL:

```
openssl x509 -inform DER -in issuer-ca.cer -out issuer-ca.pem
openssl x509 -inform DER -in va-ocsp-signing.cer -out va-ocsp-signing.pem
```

To perform the test:

1. Check that the CRL is current, is a base CRL, and contains the revoked certificate's

serial number:

```
certutil -dump issuer-ca.crl
```

2. Query the local HID VA responder, entering the revoked certificate's hexadecimal serial number with a `0x` prefix:

```
$serial = Read-Host 'Revoked certificate serial number (0x...)'
openssl ocsp -issuer issuer-ca.pem -serial $serial -url http://localhost:3501/responder -VAfile va-ocsp-signing.pem -timeout 30
```

3. Confirm the response includes **Response verify OK** and `revoked` for the expected serial number, with no response-validity errors.

Chapter 3. Additional resources and related products

3.1. nShield HSMs

3.2. nShield as a Service

3.3. Entrust products

3.4. nShield product documentation