



**ENTRUST**

**Delinea**

# Delinea Secret Server

nShield® HSM Integration Guide

2024-04-05

# Table of Contents

1. Introduction .....	1
1.1. Product configurations .....	1
1.2. Supported nShield features .....	1
1.3. Supported nShield hardware and software versions .....	2
1.4. Requirements .....	2
2. Procedures .....	4
2.1. Install the Security World software and create a Security World .....	4
2.2. Automatically start the nShield service agent at startup .....	5
2.3. Create the OCS .....	6
2.4. Enable the nShield Connect HSM .....	7
3. Additional resources and related products .....	14
3.1. Video .....	14
3.2. nShield Connect .....	14
3.3. nShield as a Service .....	14
3.4. Entrust digital security solutions .....	14
3.5. nShield product documentation .....	14

---

# Chapter 1. Introduction

Delinea Secret Server includes support for the Entrust nShield Connect Hardware Security Module (HSM). The nShield Connect HSM brings an additional layer of protection by controlling the Secret Server encryption key. This document describes the procedure to integrate Secret Server with the nShield Connect HSM.

## 1.1. Product configurations

Entrust has successfully tested nShield HSM integration with Delinea Secret Server in the following configurations:

Product	Version
Secret Server	11.6.000025 - Platinum Edition
SQL Server 2022	16.0.1000.6 Express Edition (64-bit)
SQL Server Management Studio	20.0.70.0
IIS	10.0.20348.1
Base OS	Microsoft Windows Server 2022

## 1.2. Supported nShield features

Entrust has successfully tested nShield HSM integration with the following features:

Feature	Support
Softcards	No
Module Only Key	Yes
Operator Card Set (OCS)	Yes <sup>1</sup>
nSaaS	Supported but not tested

<sup>1</sup> The OCS can only be used if it is generated without a passphrase.

Security World	Support
FIPS 140 Level 2	Yes
FIPS 140 Level 3	No

## 1.3. Supported nShield hardware and software versions

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

### 1.3.1. Connect XC

Security World Software	Firmware	Netimage	OCS	Softcard	Module
12.80.4	12.72.1 (FIPS Certified)	12.80.5	✓		✓
12.80.4	12.50.11 (FIPS Certified)	12.80.4	✓		✓
12.80.4	12.60.15 (CC Certified)	12.80.4	✓		✓

### 1.3.2. nShield 5c

Security World Software	Firmware	Netimage	OCS	Softcard	Module
13.2.2	13.2.2 (FIPS Pending)	13.2.2	✓		✓

## 1.4. Requirements

The following are needed for this integration:

- A server running Secret Server, and connected to a domain.
- A local installation of SQL or access to a remote SQL server.

- 
- An nShield Connect HSM.



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

## Chapter 2. Procedures

All steps are performed by the server that is running the Secret Server.

### 2.1. Install the Security World software and create a Security World

1. Install and configure the Security World software. For instructions, see the *Installation Guide* and the *User Guide* for the HSM.
2. Add the Security World utilities path `C:\Program Files\nCipher\nfast\bin` to the Windows system path.
3. Open port 9004 in the firewall for inbound and outbound traffic for the HSM connection.
4. Open port 9005 in the firewall for inbound and outbound traffic for remote administration using a nShield Trusted Verification Device (TVD).
5. 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](mailto:nshield.support@entrust.com).

6. Run `enquiry` to verify that the HSM is correctly configured:

```
C:\Users\Administrator>enquiry
Server
enquiry reply flags   none
enquiry reply level  Six
serial number         <ESN-of-HSM>
mode                  operational
...
Module #1
enquiry reply flags   none
enquiry reply level  Six
serial number         <ESN-of-HSM>
mode                  operational
...
```

7. Create your Security World if one does not exist already. Follow your organization's security policy for this. Create extra ACS cards, one for each person with access privilege, plus spares.

```
new-world -i -m <module_number> -Q <K/N>
```



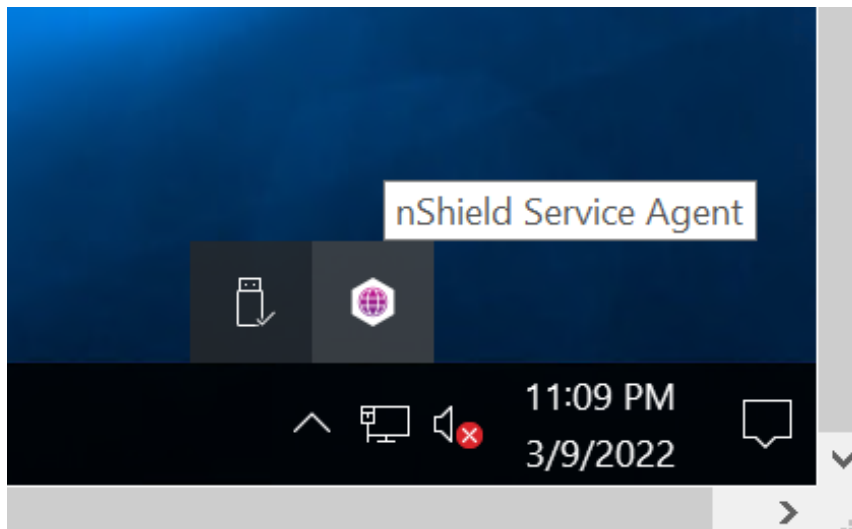
After an ACS card set has been created, the cards cannot be duplicated.

8. Run `nfkminfo` to confirm the Security World is **operational** and **usable**:

```
C:\Users\Administrator>nfkminfo
World
  generation    2
  state         0x37270008 Initialised Usable ...
  ...
Module #1
  generation    2
  state         0x2 Usable
  ...
Module #1 Slot #0 IC 0
  generation    1
  phystype      SmartCard
  ...
  error         OK
  ...
Module #1 Slot #1 IC 0
  generation    1
  phystype      SoftToken
  ...
  error         OK
  ...
```

## 2.2. Automatically start the nShield service agent at startup

1. Create a shortcut of `C:\Program Files\Cipher\ncfast\bin\nShield_service_agent.exe` and place temporarily on the desktop.
2. Select the **Windows** key + **R**, type `shell:startup`, then select **OK**.
3. Copy and paste the shortcut to the **Startup** folder.
4. Reboot.
5. Notice the nShield service agent icon shown below.



## 2.3. Create the OCS

The Secret Server private keys generated by the CNG Key storage provider can be protected with an OCS or Module only.

- OCS are smartcards that are presented to the physical smartcard reader of a HSM, or remotely via an nShield TVD. The maximum required number of cards K must be equal to 1 in the Secret Server application. The total number of cards N can be up to 64. This limit cannot be exceeded. For more information on OCS use, properties, and K-of-N values, see the *User Guide* for your HSM.
- Module protection are logical tokens with no passphrase.

Skip the remaining part of this section and go to [Enable the HSM and use CNG](#) or [Enable the HSM and use PKCS #11](#) if you are using module protection.

The following steps create the OCS. You have the option to create the OCS now or to defer creating the OCS until you configure CNG or PKCS #11.

1. Ensure that the `/opt/nfast/kmdata/config/cardlist` file contains the serial number of the card(s) to be presented or an asterisk wildcard the use of any card.
2. Open a command window as **administrator**.
3. Run `createocs`.

Press **Return** when prompted to enter a blank passphrase.

Follow your organization's security policy for the values of K/N, where K=1 as mentioned above. Use the same passphrase (left blank) for all the OCS cards in the set (one for each person with access privilege, plus spares).



---

slot 2, remote via TVD, was used to present the card in this integration.

The `-p` (persistent) option makes the authentication persist after you remove OCS card from the HSM front panel slot or from the TVD.



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

```
# createocs -m1 -s2 -N SecretServer -Q 1/1 -p

Creating Cardset:
Module 1: 0 cards of 1 written
Module 1 slot 0: Admin Card #1
Module 1 slot 2: blank card
Module 1 slot 3: empty
Module 1 slot 2:- no passphrase specified - writing card
Card writing complete.

cardset created; hkltu = 5481cad7a4b86705678e262162e95ec9318d43e6
```

4. Verify that the OCS was created:

```
# nfkminfo -c
Cardset list - 1 cardsets: (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
Operator logical token hash          k/n timeout name
5481cad7a4b86705678e262162e95ec9318d43e6 1/1 none-PL SecretServer
```

The output of `rocs` also shows the OCS:

```
# rocs
`rocs` key recovery tool
Useful commands: `help`, `help intro`, `quit`.
rocs> list cardset
No. Name                Keys (recov) Sharing
  1 SecretServer         0 (0)           1 of 1; persistent
rocs> exit
```

## 2.4. Enable the nShield Connect HSM

Use one of the options:

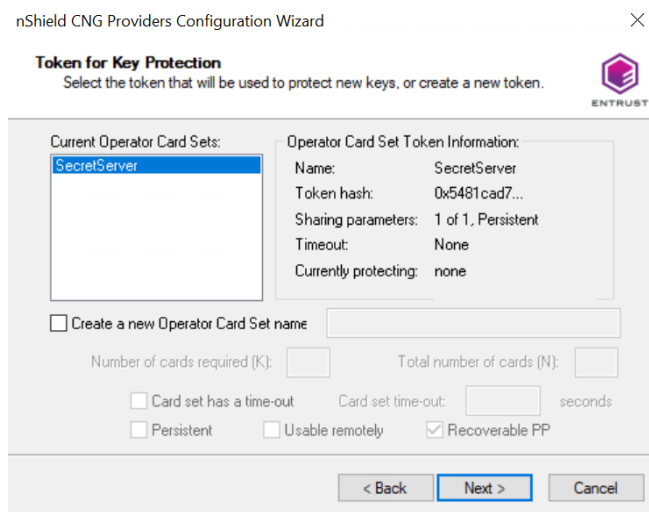
- [Enable the HSM and use CNG](#)
- [Enable the HSM and use PKCS #11](#)

### 2.4.1. Enable the HSM and use CNG

1. Select the **Windows Start > Entrust > CNG configuration** wizard.

The **nShield CNG Providers Configuration Wizard** appears.

2. Select **Next** twice.
3. Select **Use the existing security world** if one was created in [Install the Security World software and create a Security World](#).
4. Select **Next** twice.
5. Select the protection method. Either:
  - Select **Module Protection**, then select **Next** twice and then select **Finish**.
  - Select **OCS**, select the OCS created above, then select **Next** twice and then select **Finish**.



6. Run `certutil -cspstest` on a command window:

```
certutil -cspstest > <filename>
```

7. Search for **Provider Name: nCipher** in the file created above, and make sure that it shows **Pass**. For example:

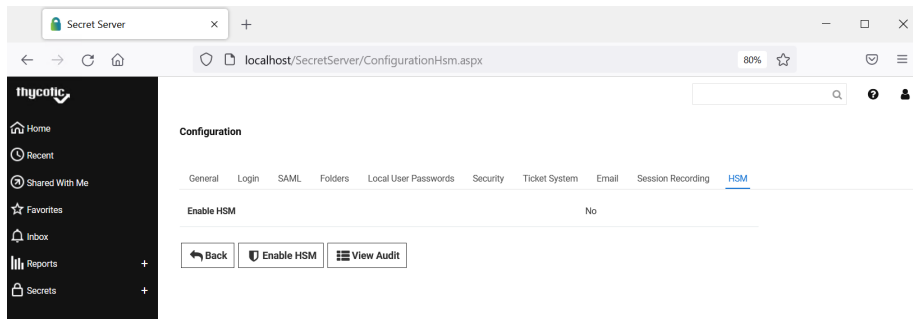
```
Provider Name: nCipher Security World Key Storage Provider
Name: nCipher Security World Key Storage Provider
HWND Handle: Binary:
0000 00 00 00 00 00 00 00 00 .....
Impl Type: 17 (0x11)
NCRYPT_IMPL_HARDWARE_FLAG -- 1
NCRYPT_IMPL_HARDWARE_RNG_FLAG -- 10 (16)

Version: 786512 (0xc0050)
Pass
...
```

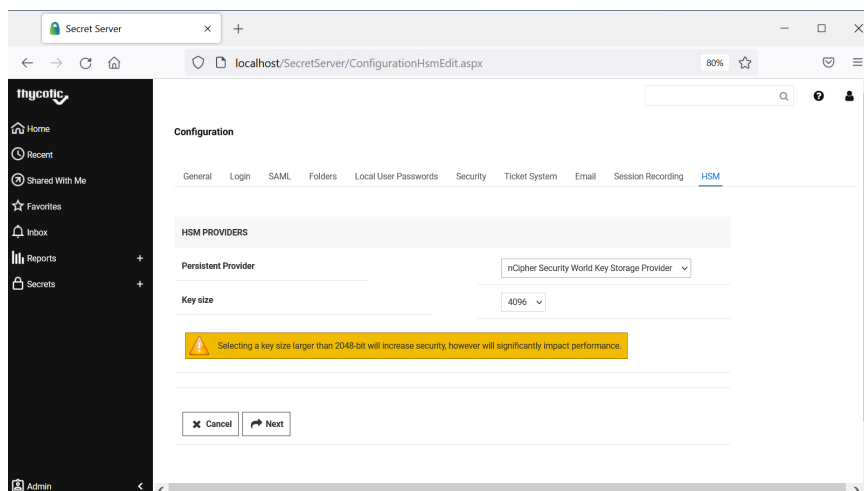
8. Log in to Delinea Secret Server via a browser at <https://localhost/SecretServer>.

- From the menu in the left pane, select **Administration > Actions > Configuration > HSM**.

The **Configuration** page appears, with the **HSM** tab selected



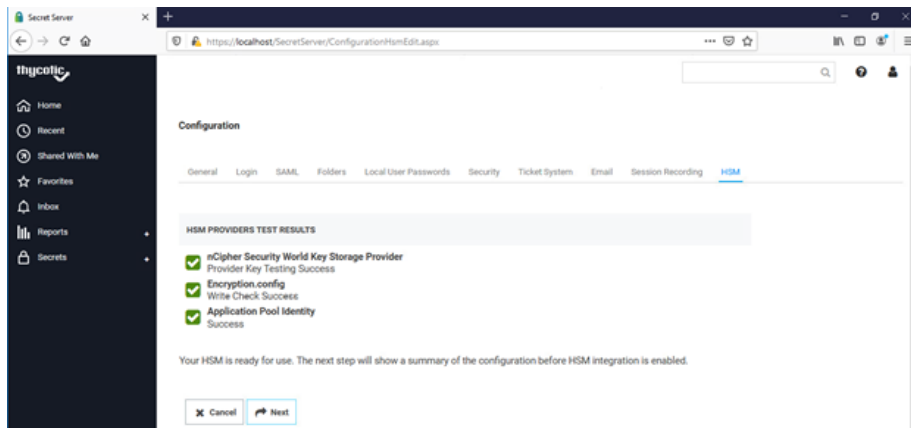
- Select **Enable HSM** and then select **Next**.
- Under **HSM Providers**:
  - For **Persistent Provider**, select **nCipher Security World Key Storage Provider**.
  - Select the required **Key size**. For example:



- Select **Next**.

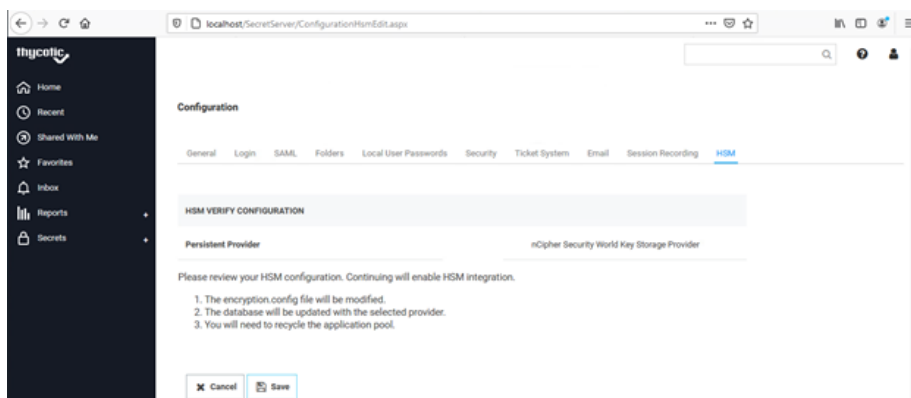
The HSM provider is tested, and results displayed.

- Check the **HSM Provider Test Results**. For example:



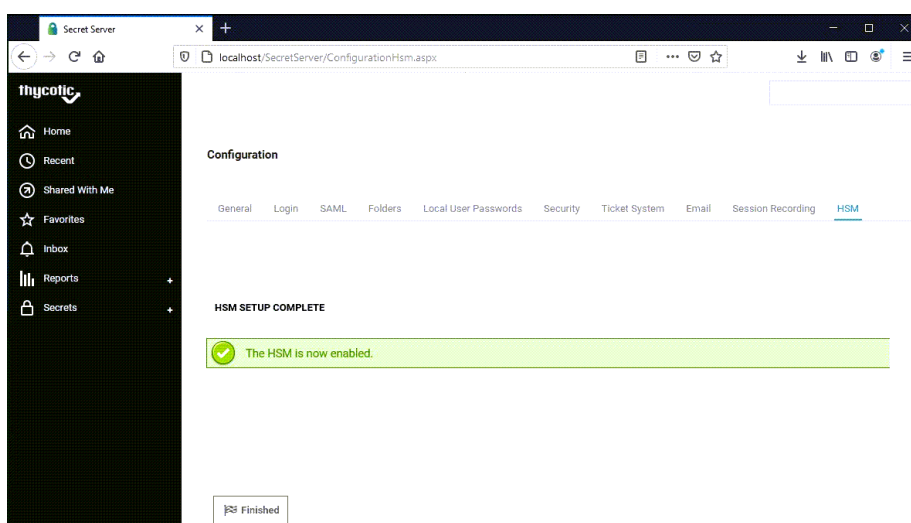
13. Select **Next**.

A verification page appears.



14. Select **Save** to update the HSM configuration.

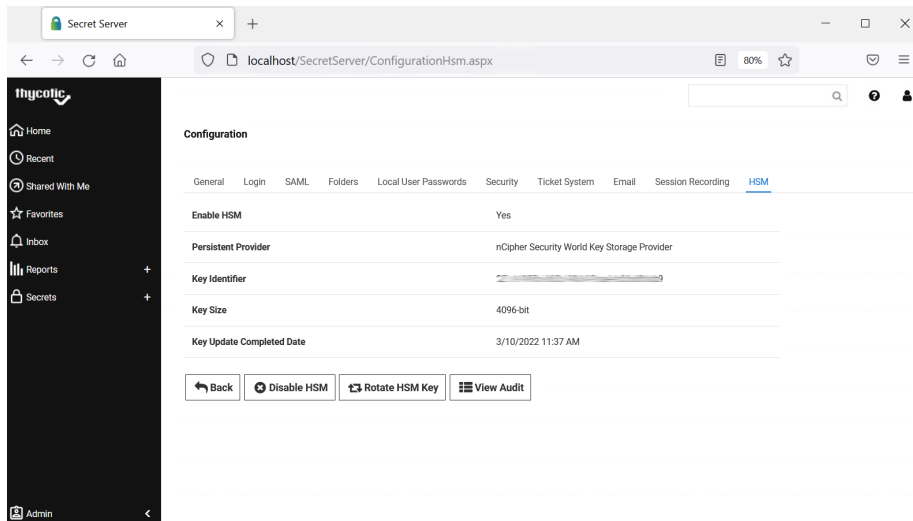
A confirmation page appears.



15. Select **Finish**.

The nShield Connect HSM is now enabled, and the Secret Server encryption

key is stored on it. The nShield Connect HSM configuration details appear on the Secret Server **HSM** tab.



## 2.4.2. Enable the HSM and use PKCS #11

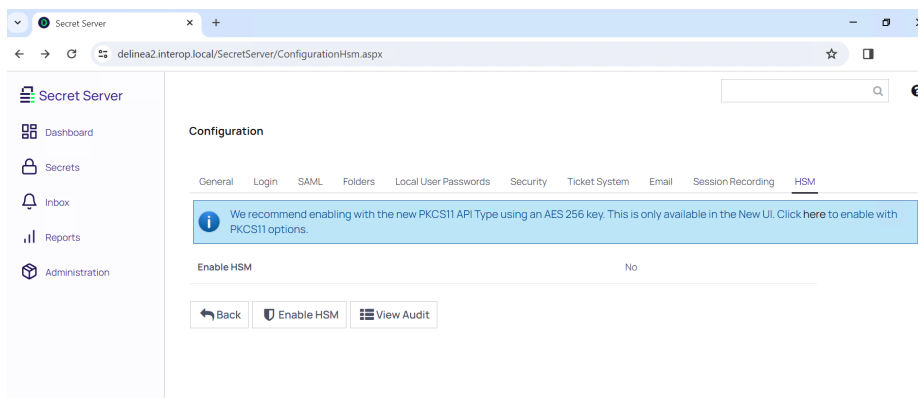
1. Copy the `cryptoki` library file

located at `C:\Program Files\nCipher\ncfast\toolkits\pkcs11\cknfast.dll`

to `C:\inetpub\wwwroot\SecretServer\pkcs11`

so that Secret Server can see it.

2. Insert your OCS card into the proper slot.
3. Select **here** in the pop up dialogue



4. For API Type, select **PKCS#11**.

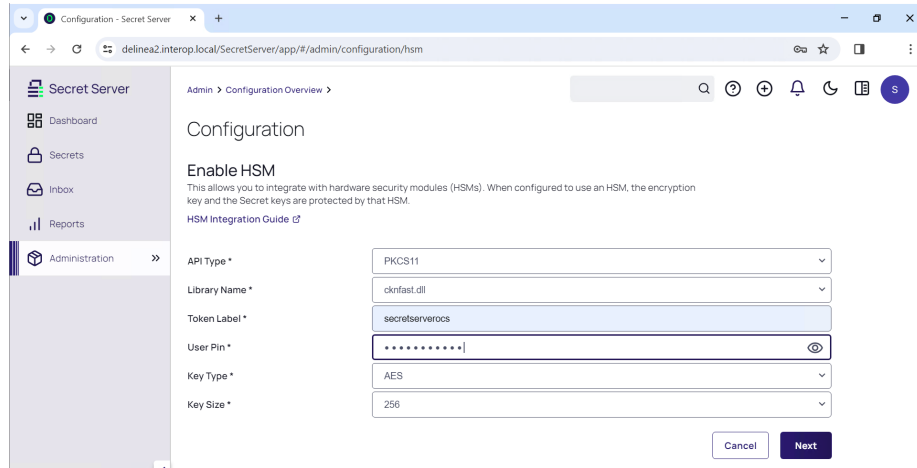
For **Library Name** select `cknfast.dll`.

For **Token Label** enter your OCS name.

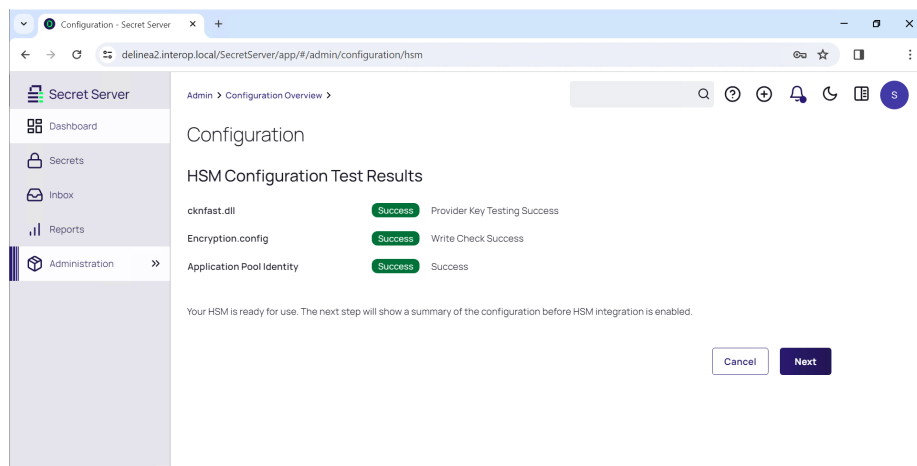
For **User Pin** enter your OCS passphrase.

Keep the default **Key Type** and **Key Size**.

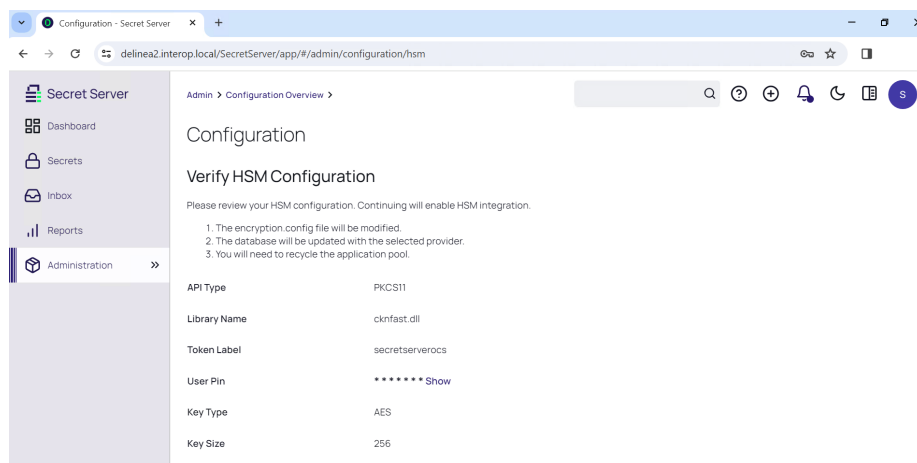
Select **Next**



5. Check the HSM Configuration Test Results, then select **Next**:



6. Verify the HSM configuration, then select **Next**



- 
7. Run `nfmverify` to verify that the key generated by the Secret Server is stored in the nShield Connect HSM:

```
C:\Users\Administrator>nfmverify

** [Security world] **
Ciphersuite: DLF3072s256mAEScSP800131Ar1
128-bit security level
1 Administrator Card(s)
  (Currently in Module #1 Slot #0: Card #1)
HKNSO 78b1cbd1814e6f711cc64fe84dae2fe3bd32584a
Cardset recovery ENABLED
Passphrase recovery ENABLED
Common Criteria CMTS 419221-5 disabled
Strict FIPS 140-2 level 3 (does not improve security) disabled
SEE application non-volatile storage ENABLED
real time clock setting ENABLED
SEE debugging ENABLED
SEE debugging restricted
Foreign Token Open authorization ENABLED
Generating module ESN <ESN-of-HSM> currently #1 (in same incarnation)

Verification successful, confirm details above. 0 keys verified.
```

This completes the integration of Delinea Secret Server with the nShield Connect HSM. Secrets created in Delinea Secret Server will use encryption keys that are stored in the nShield Connect HSM.

## Chapter 3. Additional resources and related products

[3.1. Video](#)

[3.2. nShield Connect](#)

[3.3. nShield as a Service](#)

[3.4. Entrust digital security solutions](#)

[3.5. nShield product documentation](#)