Delinea Secret Server

nShield® HSM Integration Guide

2026-10-08

© 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 features . . . 1
    1.4. Requirements . . . 2
2. Deploy and configure the Delinea Secret server . . . 3
3. Deploy and configure the nShield HSM . . . 4
    3.1. Install the nShield Security World software . . . 4
    3.2. Install the Entrust nShield HSM . . . 4
    3.3. Enroll the Entrust nShield HSM . . . 5
    3.4. Create a security world . . . 5
    3.5. Select the protection method . . . 6
    3.6. Create the OCS . . . 7
    3.7. Create the softcard . . . 8
    3.8. Automatically start the nShield service agent at startup . . . 9
4. Integrate Delinea Secret Server with an Entrust nShield HSM . . . 10
    4.1. Configure the Delinea Secret Server using the CNG cryptography provider . . . 10
    4.2. Configure the Delinea Secret Server using the PKCS #11 API . . . 15
    4.3. Verify integration . . . 19
5. Additional resources and related products . . . 21
    5.1. nShield HSMs . . . 21
    5.2. nShield as a Service . . . 21
    5.3. Entrust products . . . 21
    5.4. nShield product documentation . . . 21

Chapter 1. Introduction

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

1.1. Product configurations

Entrust has successfully tested nShield HSM integration in the following configurations:

Product	Version
Delinea Secret Server	12.2.7
SQL Server 2025	17.0.1000 Express Edition
SQL Server Management Studio 22	22.10.1
IIS	10.0.26100.32860
Base OS	Microsoft Windows Server 2025

1.2. Supported nShield hardware and software versions

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

HSM	FIPS Level	Security World	Firmware	Netimage
nShield 5c	3	v13.6.18 (LTS 8)	13.4.5 (FIPS 140-3 certified)	v13.6.18
nShield 5c	2	v13.9.6 (STS 6)	v13.8.6	v13.9.6
Connect XC	3	v13.6.18 (LTS 8)	12.72.3 (FIPS 140-2 certified)	v13.6.18
Connect XC	2	v13.9.6 (STS 6)	v13.8.5	v13.9.6

1.3. Supported nShield features

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

Feature	CNG Cryptography Provider	PKCS #11 API
Softcards	No	Yes
Module Only Key	Yes	Yes
Operator Card Set (OCS)	Yes	Yes
nSaaS	Supported but not tested	Supported but not tested

For FIPS level 3 compatibility, you need an OCS card inserted to use the Module Only Key and Softcards features.

1.4. Requirements

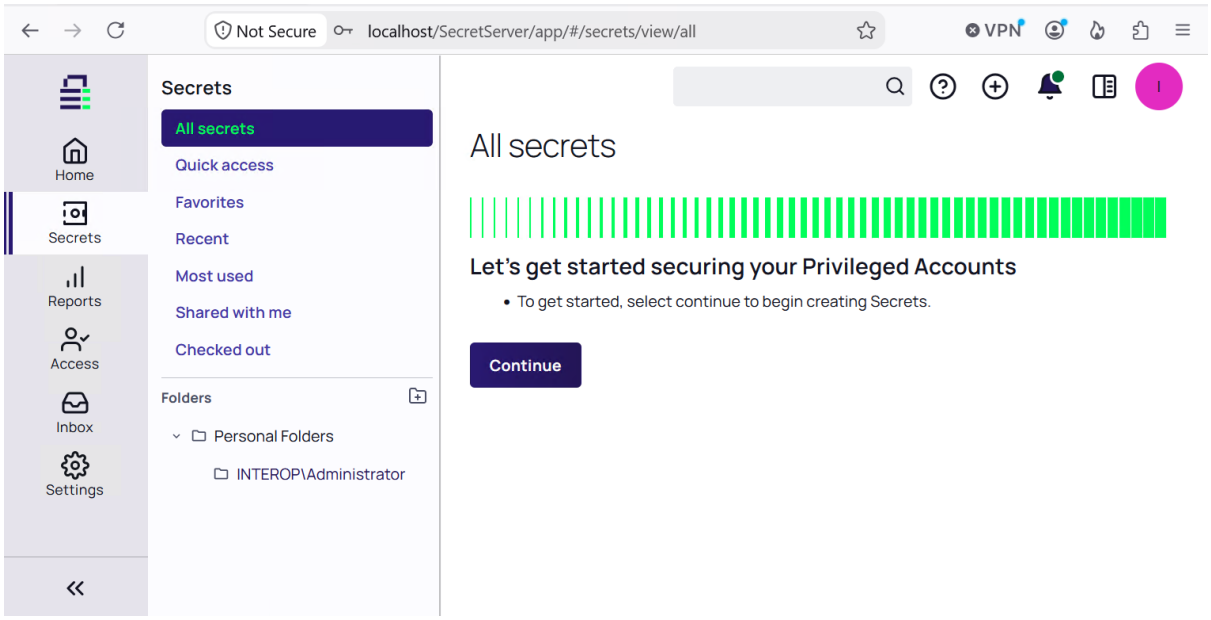
- Access to Delinea Secret Server license from your Delinea sales representative.
- Access to the Entrust TrustedCare Portal.
- An Entrust nShield HSM.
- A dedicated Windows server.
- Network environment with usable ports 9004 and 9005 for the HSM.

Familiarize yourself with the nShield Documentation.

- The importance of a correct quorum for the Administrator Card Set (ACS).
- Whether Operator Card Set (OCS) protection or Softcard protection is required.
- If OCS protection is to be used, a 1-of-N quorum must be used.
- Whether your Security World must comply with FIPS 140 Level 3 or Common Criteria standards. If using FIPS 140 Level 3, it is advisable to create an OCS for FIPS authorization. For more information see FIPS 140 Level 3 compliance.
- Whether to instantiate the Security World as recoverable or not.

Chapter 2. Deploy and configure the Delinea Secret server

Secret Server was deployed on a domain-joined Windows virtual machine. Microsoft IIS was installed on the virtual machine and configured to use the virtual machine's certificate. Secret Server was connected to an existing Microsoft SQL Server database, which was also installed on the same virtual machine. A domain-managed service account was created to support these connections. All required permissions were configured in accordance with the Delinea Documentation - Secret Server Setup.



Chapter 3. Deploy and configure the nShield HSM

All steps in this section are performed on the server hosting Secret Server.

- Install the nShield Security World software
- Install the Entrust nShield HSM
- Enroll the Entrust nShield HSM
- Create a security world
- Select the protection method

3.1. Install the nShield Security World software

1. Sign in to the Vault Server using an account with administrator privileges.
2. Install the Security World software.
   For detailed instructions, see the nShield Security World documentation.
3. Add the Security World utilities path to the system path.
   This path is typically `C:\Program Files\nCipher\nfast\bin`.
4. Run the `enquiry` utility to confirm that the Security World is in `operational` mode.

```
C:\Users\Administrator>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number
 mode                 operational
 version              13.6.18
```

5. Open firewall port 9004 for the Entrust nShield HSM connections.
6. If using Remote Administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).

3.2. Install the Entrust nShield HSM

Install the nShield HSM. Condensed instructions are available in the Entrust TrustedCare Portal.

- How To: Locally Set up a new or replacement nShield network-attached HSM.
- How To: Remotely Setup a new or replacement nShield network-attached HSM.
- How To: Remotely Setup a new or replacement nShield Connect XC Serial Console

Model.

For detailed instructions see the Hardware install and setup guides.

3.3. Enroll the Entrust nShield HSM

1. Inform the HSM of the location of the Vault Server.

   For instructions, see Configuring the nShield HSM to use the client.

   If you are using a high-availability setup, repeat the client configuration for each HSM.

2. Enroll the Vault Server as a client of the HSM.

   For instructions, see Configuring client computers to use the nShield HSM.

   If you are using a high-availability setup, repeat the enrollment for each HSM.

3. Run the `enquiry` utility to confirm that the HSM is in `operational` mode.

```
C:\Users\Administrator>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        6A74-1261-7843 810B-03E0-D947
 mode                 operational
 version              13.6.18
...
Module #1:
 enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        6A74-1261-7843
 mode                 operational
 version              13.4.5
 ...
Module #2:
 enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        810B-03E0-D947
 mode                 operational
 version              12.72.4
```

3.4. Create a security world

1. Create a new Security World, if one does not already exist, or copy an existing one.

   Follow your organization's security policy for this. For more information see Create a new Security World.

   ACS cards cannot be duplicated after the Security World is created. You may want to create extras in case of a card failure or a

> lost card.

2. Confirm the Security World is in a `Usable` state with the `nfkminfo` utility.

```
C:\Users\Administrator>nfkminfo
World
 generation  2
 state       0x3737000c Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
Module #2
 generation 2
 state      0x2 Usable
```

3.5. Select the protection method

The following protection methods are available to authorize access to Secret Server keys protected by the HSM.

- An Operator Card Set (OCS) is a set of smartcards that are presented to the physical smartcard reader of an HSM. For more information on OCS use, properties, and K-of-N values, see Operator Card Sets (OCS).
- Softcards are logical tokens (passphrases) that protect the key and authorize its use. For more information on softcard use, see Softcards.
- Module protected keys are simply protected by a module key. For more information on module protection, see Module protection.

Follow your organization's security policy to select an authorization access method.

Depending on the protection method select, you may need to define some environment variables. You have the option to set these environment variables with the Windows `set` command, or edit file `C:\Program Files\nCipher\nfast\cknfastrc`. The Windows `set` command is preferred. As reference, all environment variables are listed in nShield PKCS #11 library environment variables.

Enable softcard protection:

```
C:\Users\Administrator.INTEROP>set CKNFAST_LOADSHARING=1
```

Enable module protection:

```
C:\Users\Administrator.INTEROP>set CKNFAST_FAKE_ACCELERATOR_LOGIN=1
```

Sample `C:\Program Files\nCipher\nfast\cknfastrc` file:

```
# Enable Softcard protection
CKNFAST_LOADSHARING=1

# Enable Module protection
CKNFAST_FAKE_ACCELERATOR_LOGIN=1

# OCS Preload file location
# Un-comment the next line ONLY in using preload
#NFAST_NFKM_TOKENSFILE="C:\Program Files\nCipher\nfast\preloadtoken"
```

3.6. Create the OCS

The OCS quorum and passphrase must be set as shown next.

Feature	CNG Cryptography Provider	PKCS #11 API
Quorum K	1	1
Passphrase	None. Left blank	<passphrase>

Recovering from a power failure requires the OCS to be inserted in the HSM or the TVD.

1. Ensure file `/opt/nfast/kmdata/config/cardlist` 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. Create the OCS as described in Create Operator Card Sets (OCSs).

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

   In the example below, `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 testOCSnopassphrase -Q 1/1
   ```

4. Verify that the OCS was created.

```
C:\Users\Administrator.INTEROP>nfkminfo -c
Cardset list - 2 cardsets:  (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
 Operator logical token hash               k/n timeout  name
 7aaf758bc6790206198ea5218040d4faa09f035f  1/5  none-NL testOCSnopassphrase
 edb3d45a28e5a6b22b033684ce589d9e198272c2  1/5  none-NL testOCS
```

The `rocs` utility also shows the OCS created.

```
C:\Users\Administrator.INTEROP>rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cardset
No. Name                    Keys (recov) Sharing
  1 testOCSnopassphrase     0 (0)        1 of 5
  2 testOCS                 1 (1)        1 of 5
rocs> exit
```

3.7. Create the softcard

1. Enable softcard protection as described in Select the protection method.
2. Open a command window as an administrator.
3. Create the softcard as described in Create softcards.

   For example

```
# ppmk -n testSC
```

4. Verify the softcard.

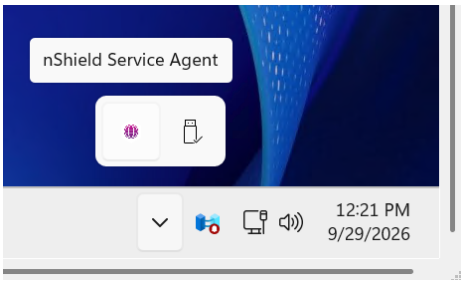
```
# nfkminfo -s
SoftCard summary - 1 softcards:
 Operator logical token hash               name
 9252345678923456234567897bde3753d24e7744  testSC
```

The `rocs` utility also shows the new softcard.

```
# rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cards
No. Name                    Keys (recov) Sharing
  1 testOCS                 0 (0)        1 of 5
  2 testSC                  0 (0)        (softcard)
rocs> quit
```

3.8. Automatically start the nShield service agent at startup

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



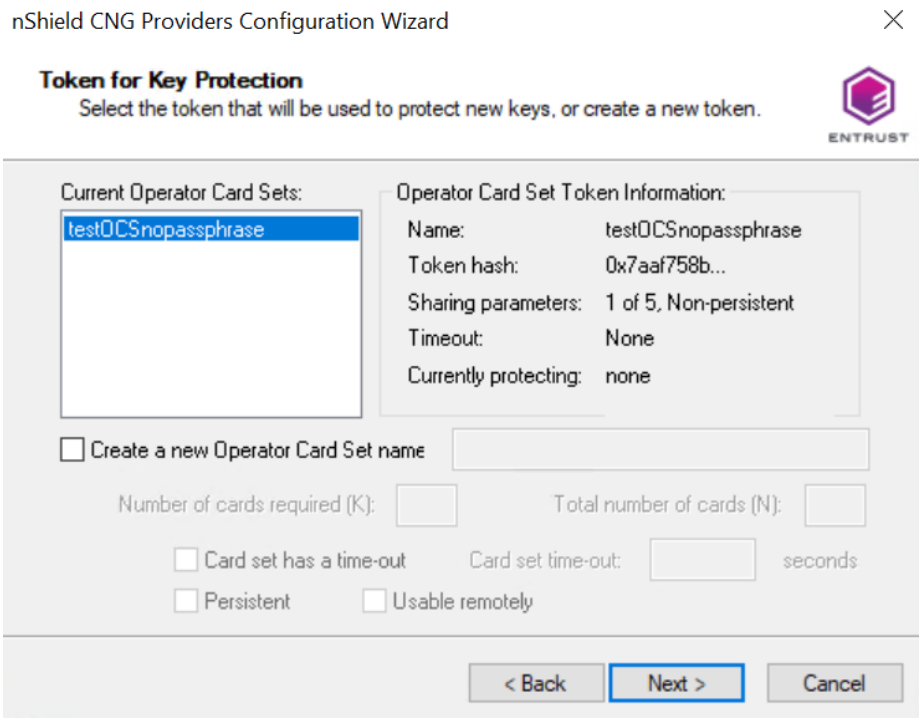
Chapter 4. Integrate Delinea Secret Server with an Entrust nShield HSM

There are two cryptography API options for this integration: the CNG cryptography provider, and the PKCS #11. Both are covered in this section.

4.1. Configure the Delinea Secret Server using the CNG cryptography provider

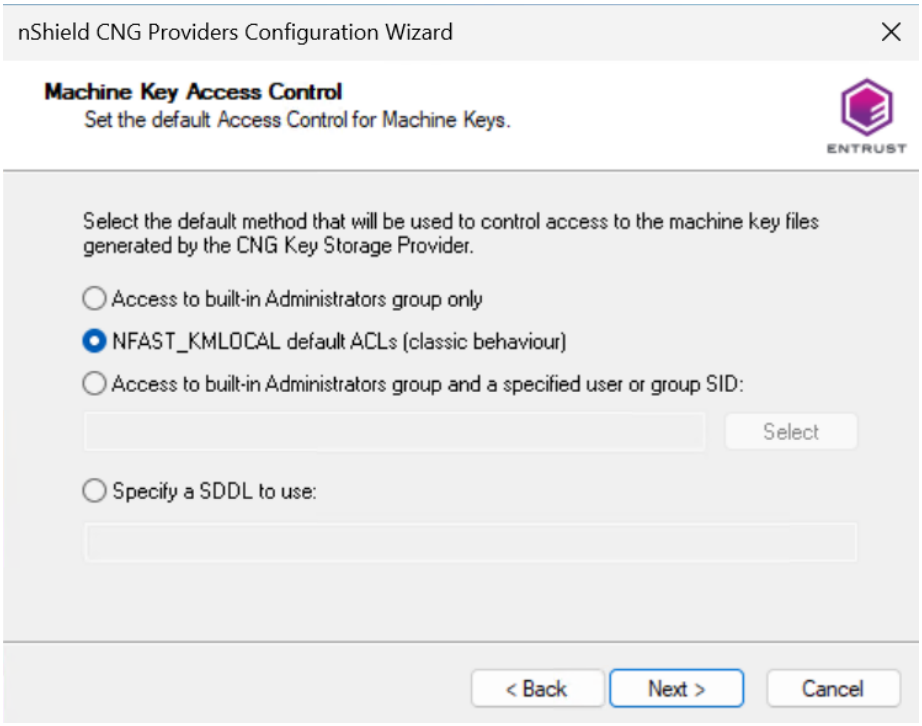
1. Select **Windows Start > Entrust nShield Security World > CNG configuration wizard**. The **nShield CNG Providers Configuration Wizard** appears.
2. Select **Next** twice.
3. Select **Use the existing security world** if one was created in Create a Security World.
4. Select **Next** twice.
5. Select the protection method. If you are using OCS protection, insert your OCS card into the proper slot and then select **Next**.

   Example for OCS protection:



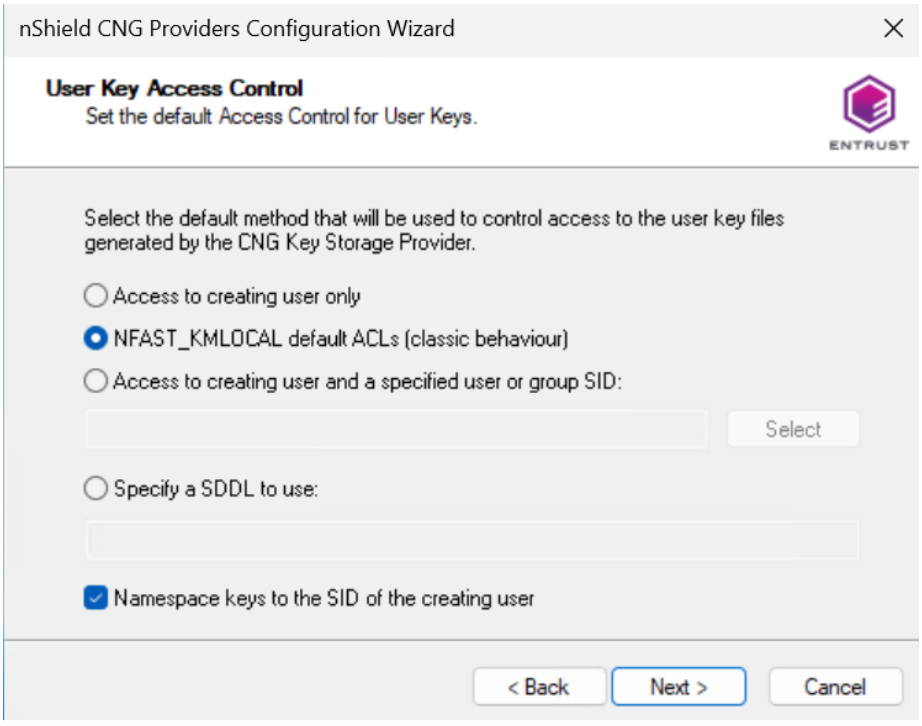
6. If the **Machine Key Access Control** window appears, select the option that best meets your security and operational requirements and specify the service account used by the Secret Server, then select **Next**.

For example:



7. If the **User Key Access Control** window appears, select the option that best meets your security and operational requirements and ensure that the **Namespace keys to the SID of the creating user** remains selected, then select **Next**.

   For example:

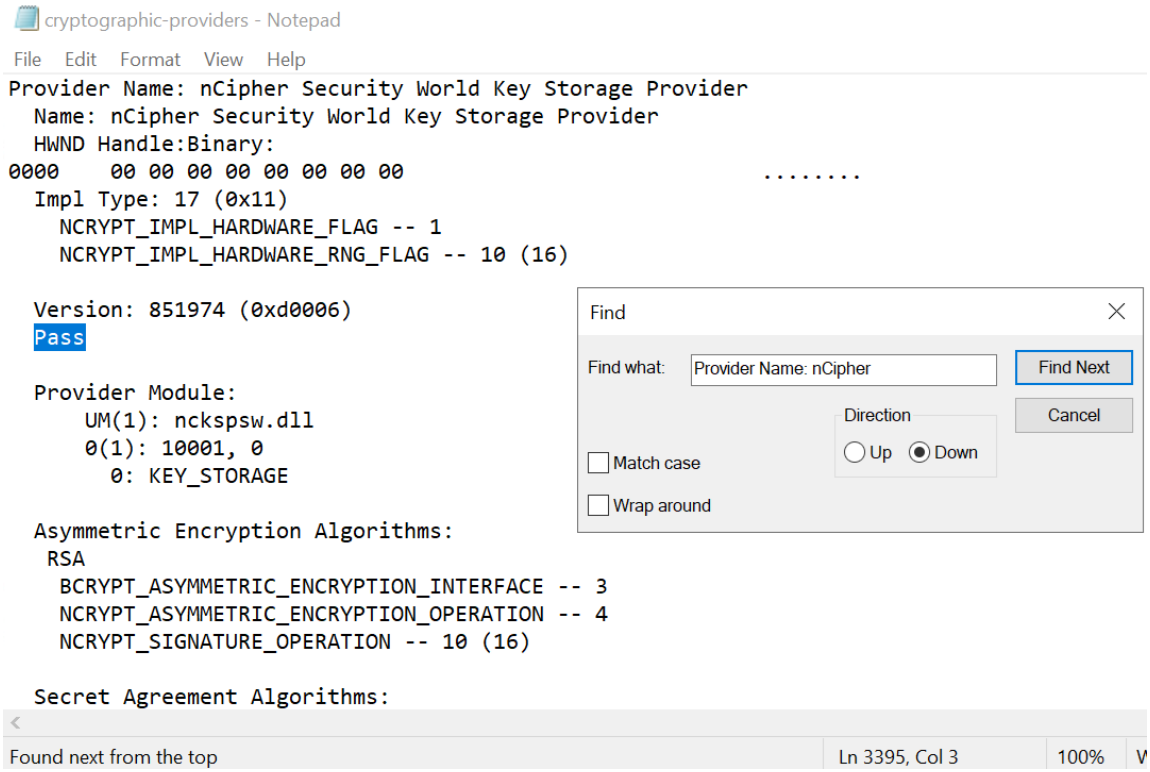


8. Select **Next** and **Finish**.
9. Run `certutil -csptest > <filename>` on a command window.

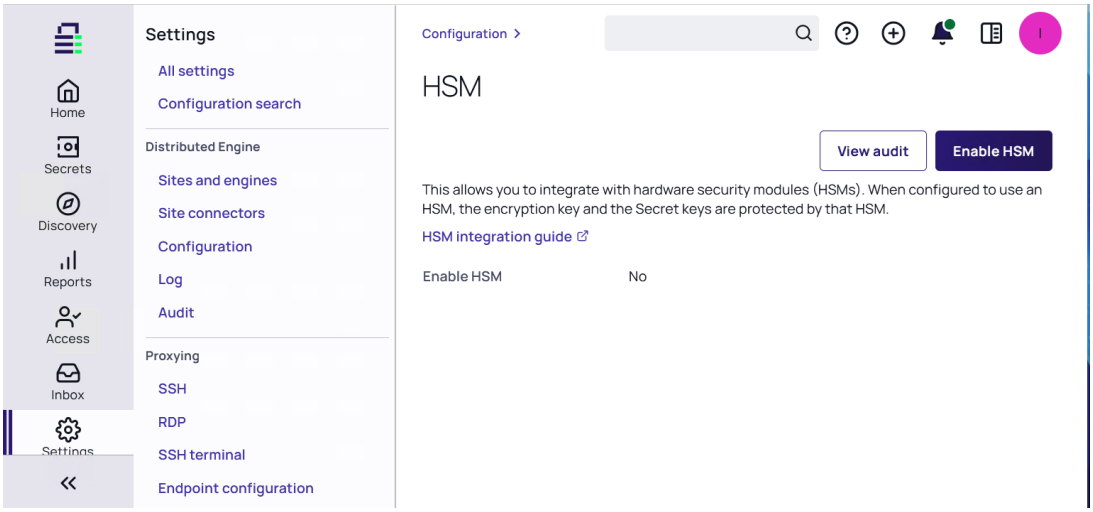
   For example:

   ```
   C:\Users\Administrator.INTEROP>certutil -csptest > Documents\cryptographic-providers
   ```

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



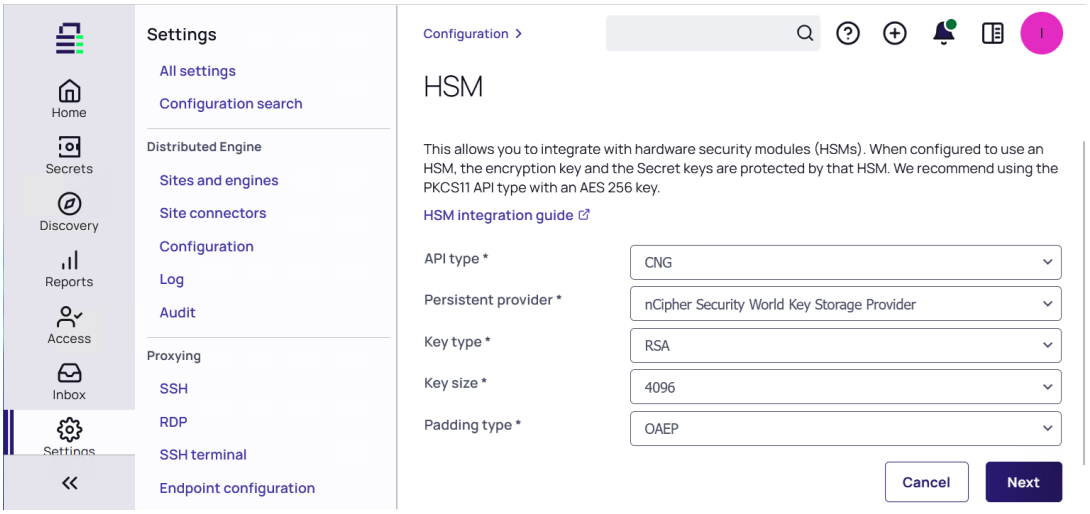
11. Log in to the Delinea Secret Server via a browser at https://localhost/SecretServer.
12. From the menu in the left pane, select **Settings > All settings > Configuration > General > HSM**. The **HSM configuration** page appears.



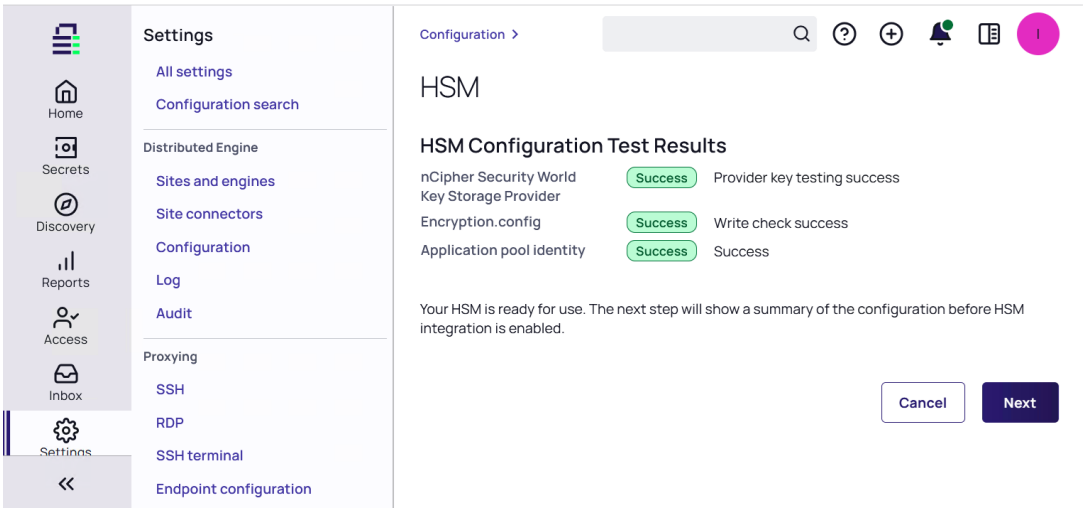
13. Select **Enable HSM**, then select **Next**.
14. In the **Enable HSM** window, select as follows, then select **Next**.

Parameter	Value
API type	Select **CNG**
Persistent provider	Select **nCipher Security World Key Storage Provider**
Key type	Select the required value
Key size	Select the required value
Padding type	Select the required value

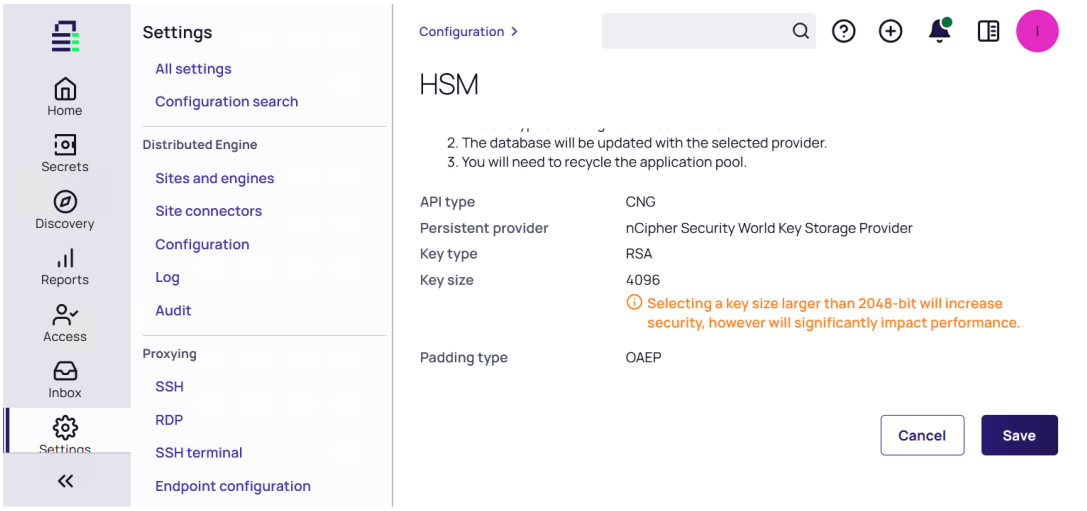
For example:



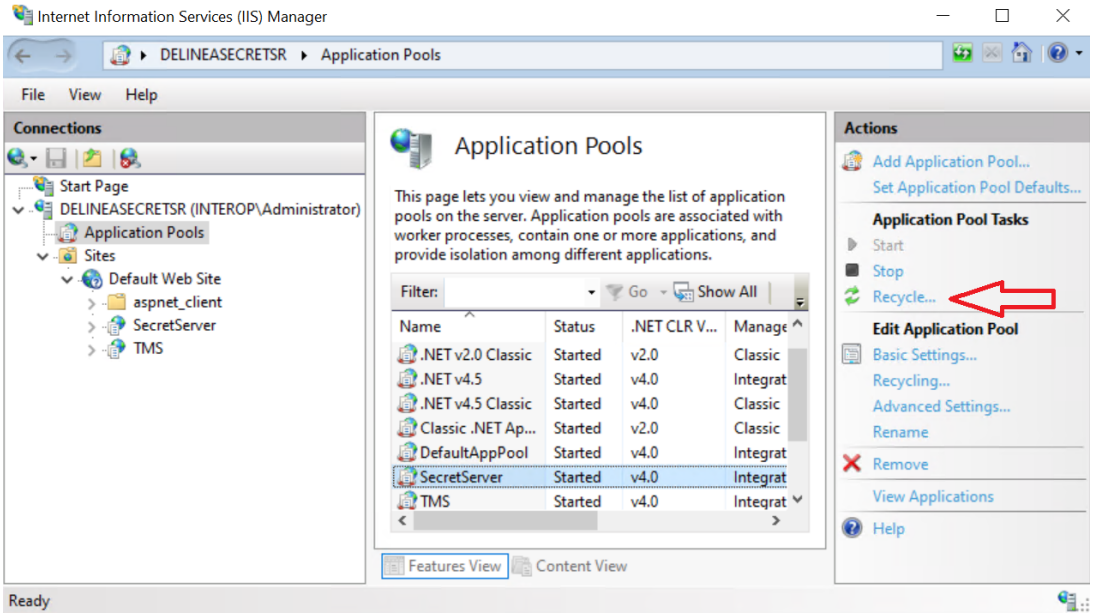
15. Check the **HSM Provider Test Results**, then select **Next**.



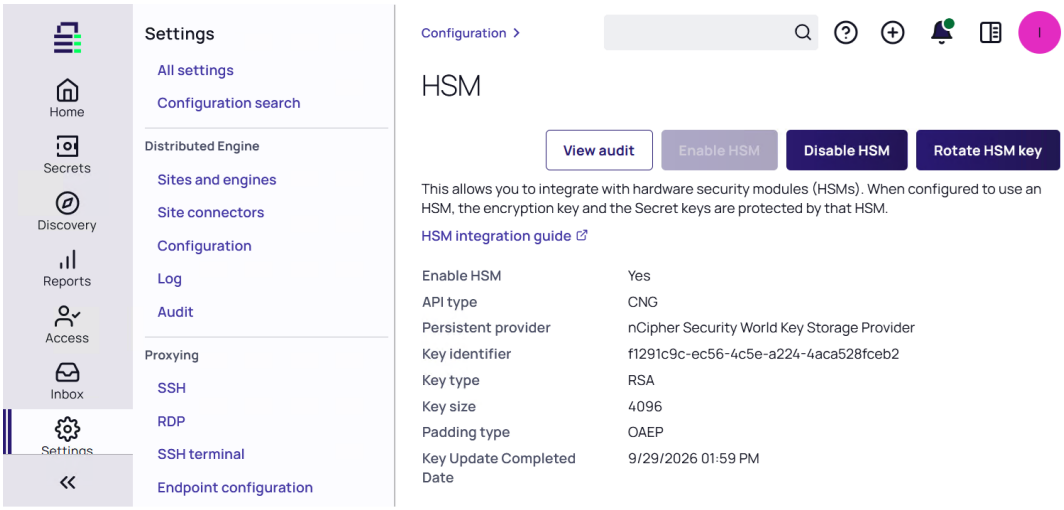
16. In the **Verify HSM configuration** page select **Save**.



17. In the **Notice** about HSM configuration change, recycle the application pool and then select **Continue**.



18. Refresh the browser. Then from the menu in the left pane, select **Settings > All settings > Configuration > General > HSM**. Notice the completed HSM configuration.



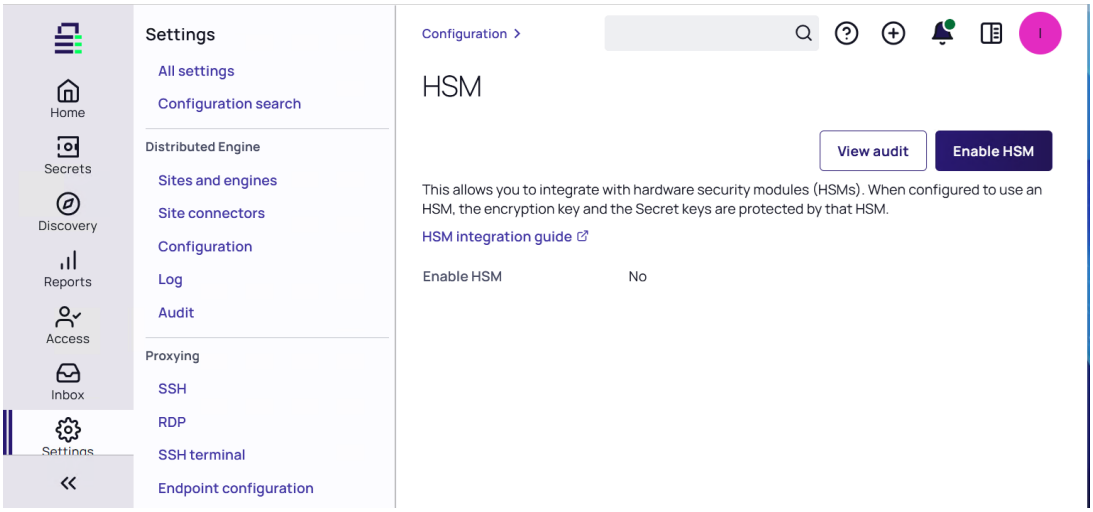
4.2. Configure the Delinea Secret Server using the PKCS #11 API

1. Log in to the Delinea Secret Server via a browser at https://localhost/SecretServer.
2. Copy the HSM `cryptoki` library (dll) for PKCS #11 to the Secret Sever application pool as shown:

```
C:\Users\Administrator.INTEROP>mkdir C:\inetpub\wwwroot\SecretServer\pkcs11

C:\Users\Administrator.INTEROP>copy "C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll"
C:\inetpub\wwwroot\SecretServer\pkcs11\.
        1 file(s) copied.
```

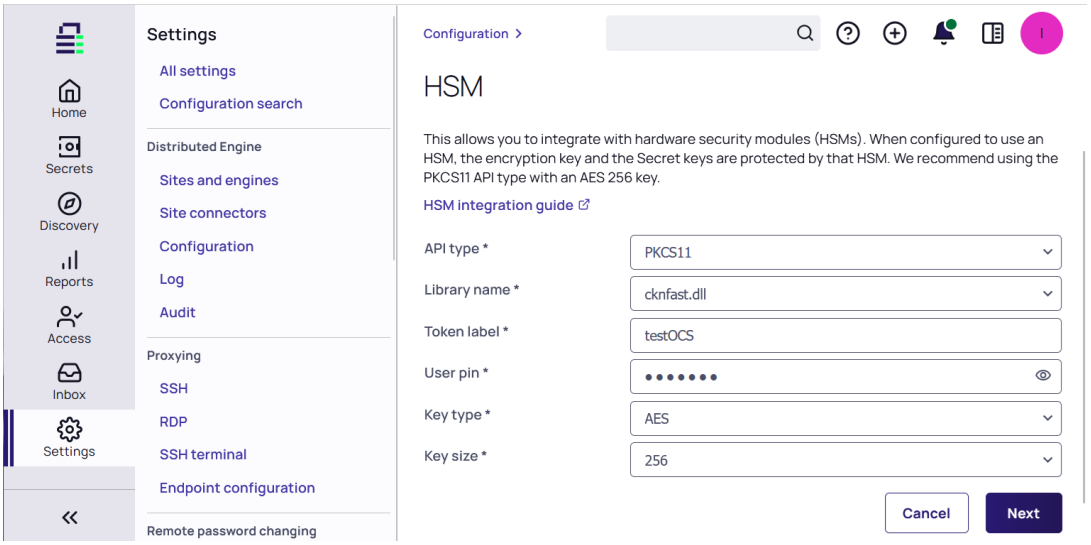
3. If you are using OCS protection, insert your OCS card into the proper slot.
4. From the menu in the left pane, select **Settings > All settings > Configuration > General > HSM**. The **HSM configuration** page appears.



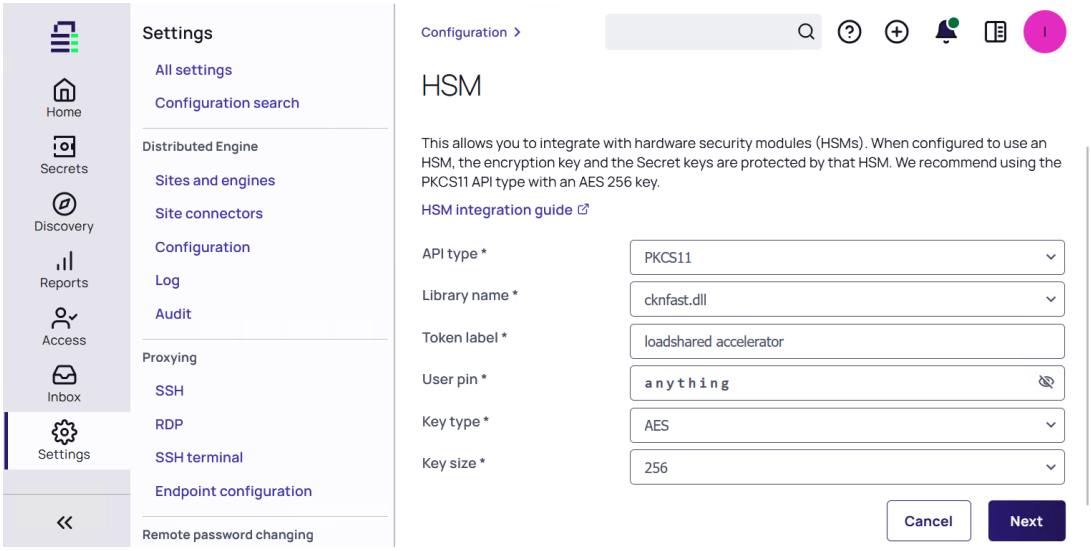
5. Select **Enable HSM**, then select **Next**.
6. In the **Enable HSM** window, complete the fields as follows, then select **Next**.

Parameter	Value
API type	Select **PKCS11**
Library name	Select **cknfast.dll**
Token label	Enter the token name
User pin	Enter the token passphrase
Key type	Select the required value
Key size	Select the required value

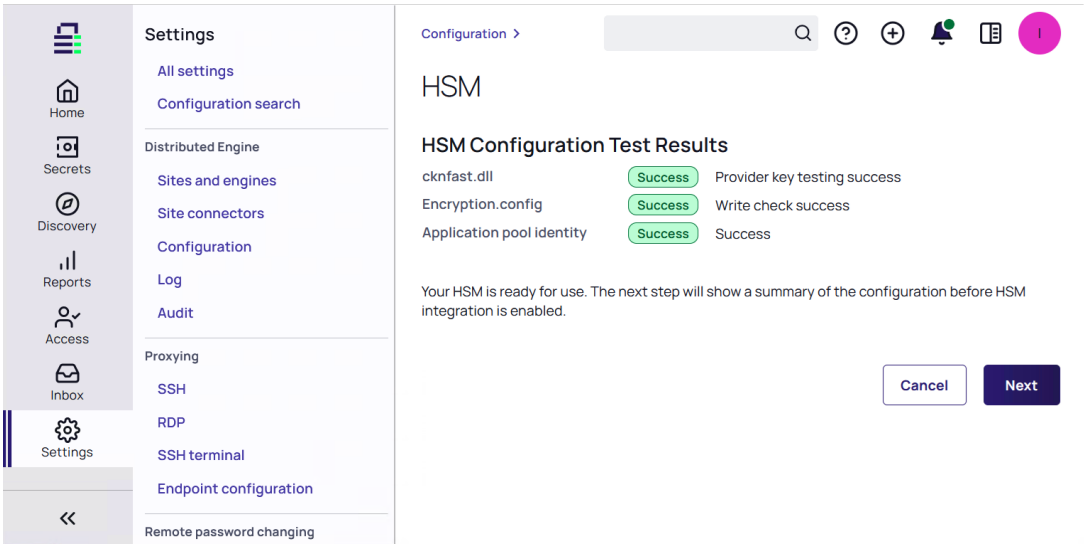
Example with OCS protection:



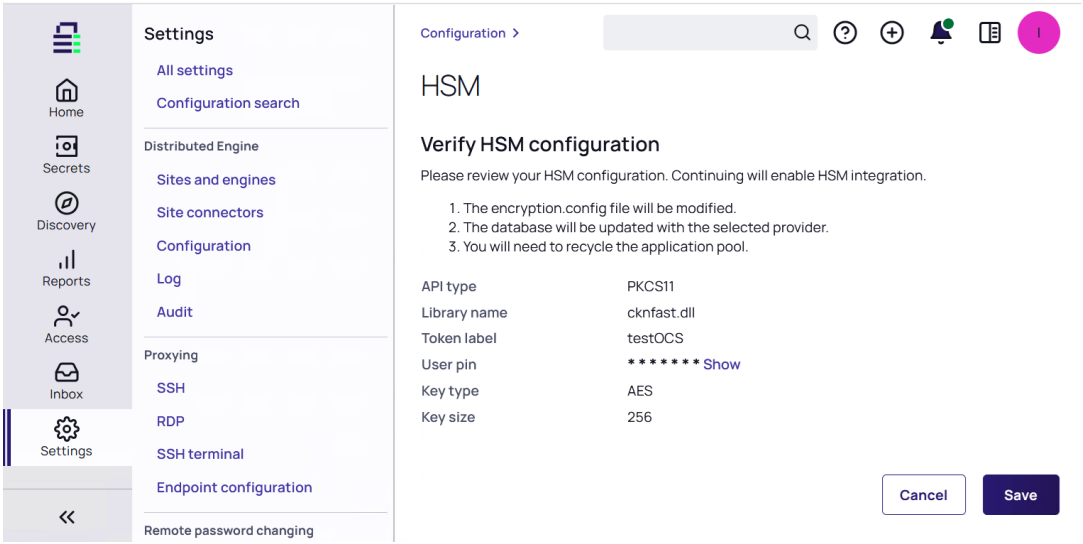
Example with module-only protection:



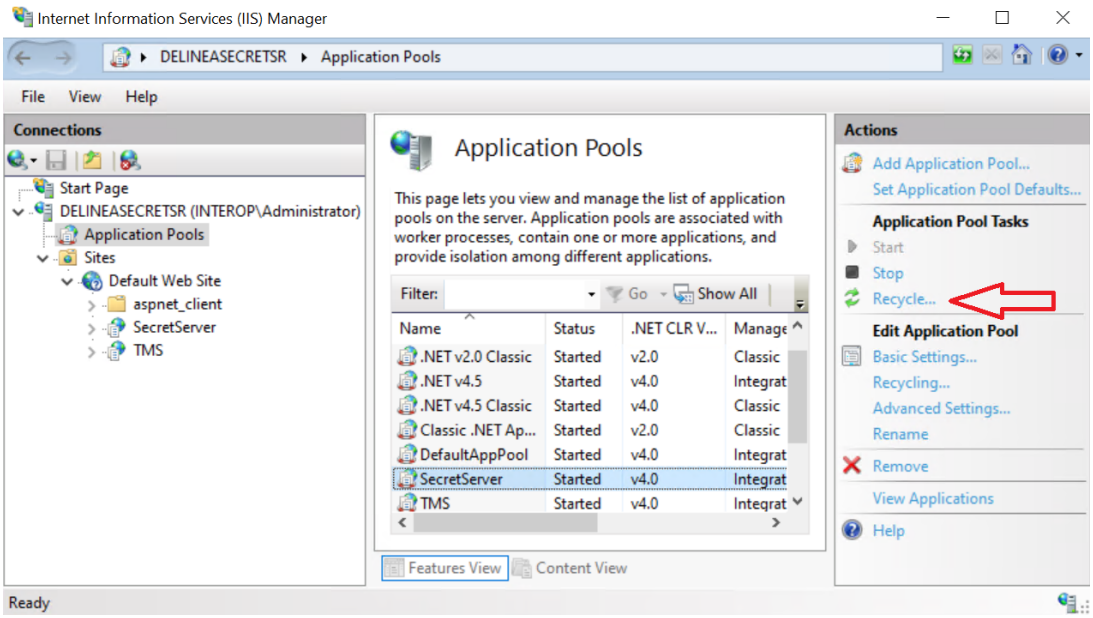
7. Check the **HSM Provider Test Results**, then select **Next**.



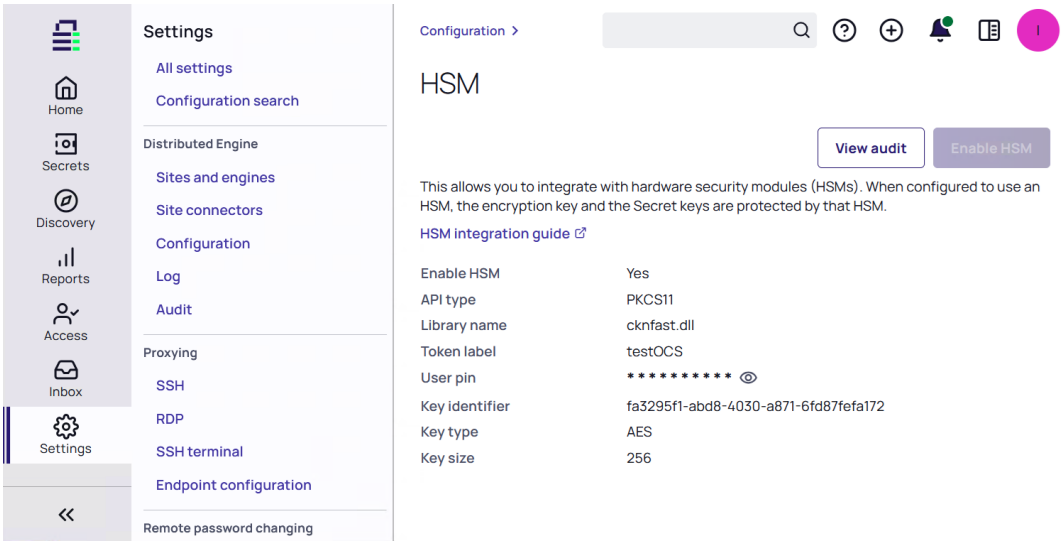
8. In the **Verify HSM configuration** page select **Save**.



9. In the **Notice** about HSM configuration change, recycle the application pool and then select **Continue**.



10. Refresh the browser. Then from the menu in the left pane, select **Settings > All settings > Configuration > General > HSM**. Notice the completed HSM configuration.



4.3. Verify integration

1. List the keys protected by the HSM using the `nfkminfo` and `rocs` utilities.
   For example:

   - A key using the CNG cryptography provider:

```
C:\Users\Administrator.INTEROP>nfkminfo -l

Keys protected by cardsets:
 key_caping_s-1-5-21-113020180-2446387811-180773374-1216--0d2944734a6e884bebffa501ccf26757dc717596
`f1291c9c-ec56-4c5e-a224-4aca528fceb2'

C:\Users\Administrator.INTEROP>rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list keys
  No. Name                    App        Protected by
    1 f1291c9c-ec56-4c5e-a224- caping     testOCSnopassphrase
rocs> quit
```

   - A key using the PKCS #11 API:

```
C:\Users\Administrator.INTEROP>nfkminfo -l

Keys protected by cardsets:
 key_pkcs11_ucedb3d45a28e5a6b22b033684ce589d9e198272c2-7138a95db0d16a7e8cbe97e4ac6e201002e33b73
`fa3295f1-abd8-4030-a871-6fd87fefa172'

C:\Users\Administrator.INTEROP>rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list keys
  No. Name                    App        Protected by
    1 fa3295f1-abd8-4030-a871- pkcs11     testOCS
rocs> exit
```

2. Notice the **Key identifier** in the completed HSM configuration matches the `nfkminfo` utility output above.

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

Chapter 5. Additional resources and related products

5.1. nShield HSMs

5.2. nShield as a Service

5.3. Entrust products

5.4. nShield product documentation