



Delinea Secret Server

nShield[®] HSM Integration Guide

2025-04-14

© 2025 Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction
1.1. Product configurations
1.2. Supported nShield features
1.3. Supported nShield hardware and software versions
1.4. Requirements
2. Deploy and configure the Entrust nShield HSM
2.1. Install the Security World software and create a Security World
2.2. Automatically start the nShield service agent at startup
2.3. Create the OCS
3. Integrate Delinea Secret Server with an Entrust nShield HSM7
3.1. Configure the Delinea Secret Server using the CNG cryptography provider7
3.2. Configure the Delinea Secret Server using the PKCS #11 API
3.3. Verify integration
4. Additional resources and related products
4.1. nShield Connect
4.2. nShield as a Service
4.3. Entrust products
4.4. nShield product documentation

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 Delinea Secret Server encryption key. This document describes the procedure to integrate Delinea 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
Delinea 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	CNG Cryptography Provider	PKCS #11 API
Softcards	No	Yes
Module Only Key	Yes	Yes
Operator Card Set (OCS)	Yes but without a passphrase	Yes
nSaaS	Supported but not tested	Supported but not tested

Security World	Support
FIPS 140 Level 2	Yes
FIPS 140 Level 3	Yes

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 140-2 certified)	12.80.5	\checkmark		\checkmark
12.80.4	12.50.11 (FIPS 140-2 certified)	12.80.4	\checkmark		\checkmark
12.80.4	12.60.15 (CC certified)	12.80.4	\checkmark		\checkmark
13.4.4	12.50.11 (FIPS 140-2 certified)	12.80.4	\checkmark		\checkmark

1.3.2. nShield 5c

Security World Software	Firmware	Netimage	OCS	Softcard	Module
13.2.2	13.2.2	13.2.2	\checkmark		\checkmark

1.4. Requirements

The following are needed for this integration:

- A server running Delinea Secret Server.
- An nShield Connect HSM.

Chapter 2. Deploy and configure the Entrust nShield HSM

All steps below are performed in the server running the Secret Server.

- Install the Security World software and create a Security World
- Automatically start the nShield service agent at startup
- Create the OCS

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.

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

C:\Users\Admin Server	istrator>@	enquiry
enquiry reply	flags	none
enquiry reply	level	Six
serial number		<esn-of-hsm< td=""></esn-of-hsm<>
mode		operational
 Module #1		

enquiry reply flags	none
enquiry reply level	Six
serial number	<esn-of-hsm></esn-of-hsm>
mode	operational

 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
             0x37270008 Initialised Usable ...
state
Module #1
generation 2
            0x2 Usable
state
. . .
Module #1 Slot #0 IC 0
generation 1
phystype
             SmartCard
 . . .
             OK
еггог
Module #1 Slot #1 IC 0
 generation 1
             SoftToken
 phystype
 . . .
              0K
еггог
. . .
```

2.2. 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. 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 Delinea Secret Server private keys generated by the Entrust nShield HSM can be protected with Softcard, module-only, and OCS as described in section Supported nShield features.

- OCS are smartcards that are presented to the physical smartcard reader of a HSM, or remotely via an nShield trusted verification device (TVD). The quorum K must be equal to 1 in the Secret Server application. For more information on OCS use, properties, and K-of-N values, see the User Guide for your HSM.
- · Softcards are logical tokens protected with a passphrase.
- Module-only are logical tokens with no passphrase.

The examples shown in this integration guide use OCS protection. The following steps create the OCS.

- 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. 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 with CNG) 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:

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
```

Chapter 3. Integrate Delinea Secret Server with an Entrust nShield HSM

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

- Configure the Delinea Secret Server using the CNG cryptography provider
- Configure the Delinea Secret Server using the PKCS #11 API
- Verify integration

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

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.

nShield CNG Providers Configuration Token for Key Protection Select the token that will be used	Wizard to protect new keys, or o	create a new token.	K
Current Operator Card Sets: SecretServer	 Operator Card Set Tol Name: Token hash: Sharing parameters: Timeout: Currently protecting: 	ken Information: SecretServer 0x5481cad7 1 of 1, Persistent None none	
Create a new Operator Card Set Number of cards required (K): Card set has a time Persistent	name Tota	al number of cards (N): out:se V Recoverable PP	conds
	< Back	Next >	Cancel

6. Run certutil -csptest on a command window:

certutil -csptest > <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

Secret Server	× +		-		×
\leftarrow \rightarrow C \textcircled{a}	O D localhost/SecretServer/ConfigurationHsm.aspx 80%	☆		\bigtriangledown	≡
thycotic.			Q	0	4
合Home	Configuration				
() Recent					
O Shared With Me	General Login SAML Folders Local User Passwords Security Ticket System Email Session Recording HSM				
☆ Favorites	Enable HSM No				
ậ Inbox					
Reports +	Sack				
A Secrets +					

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

	Secret Server	× +	-		×
\leftarrow	\rightarrow C \textcircled{a}	🔿 🗅 localhost/SecretServer/ConfigurationHsmEdit.aspx 80% 🏠	3	\bigtriangledown	≡
thyc	otic		Q	0	a ^
ᡬᡆ _{Hor}	ne	Configuration			
C Rec	ent				
闭 Sha	red With Me	General Login SAML Folders Local User Passwords Security Ticket System Email Session Recording			
☆ Fav	orites				
¢ Inbo	ж	HSM PROVIDERS			
Rep	orts +	Persistent Provider nCinhor Security World Key Storane Provider			
🖰 Sec	rets +	respire occurry non-regioninger romaine -			
		Key size 4096 v			
		Selecting a key size larger than 2048-bit will increase security, however will significantly impact performance.			
		X Cancel			
홉 Adr	nin <	<			>

c. Select Next.

The HSM provider is tested, and results displayed.

12. Check the HSM Provider Test Results. For example:

🔒 Secret Server

thycotic,

Gi Home

() Recent (3) Shared W

Reports

A Secrets

☆ <u>∆</u> Inbox

13. Select Next.

A verification page appears.

🗶 Cancel 🥐 Next

€ → ୯ û	localhost/SecretServer/ConfigurationHsmEdit.aspx	☺ ☆	lin © 😻 ≣
thycotic,			َ و ه أ
Gir Home			
(Recent	Configuration		
Shared With Me			
🛱 Favorites	General Login SAML Folders Local User Passwords Security Ticket System Email Session Record	ang HSM	
⊈ Inbox			
III Reports +	HSM VERIFY CONFIGURATION		
🛆 Secrets +	Persistent Provider nCipher Security World Key Storage Prov	ider	
	Please review your HSM configuration. Continuing will enable HSM integration.		
	1. The encryption config file will be modified.		
	2. The database will be updated with the selected provider. 3. You will need to recycle the application pool.		
	X Cancel (5) Save		

Your HSM is ready for use. The next step will show a summary of the configuration before HSM integration is enabled.

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

A confirmation page appears.

Secret Server	× +	- 🗆 ×
← → ♂ ŵ	0 Coalhost/SecretServer/ConfigurationHsm.aspx	
thycotic.		
G Home		
C Recent	Configuration	
Shared With Me		
☆ Favorites	General Login SAML Folders Local User Passwords Security	Ticket System Email Session Recording HSM
🗘 Inbox		
Reports	•	
A Secrets	+ HSM SETUP COMPLETE	
	The HSM is now enabled.	

15. Select Finish.

The nShield Connect HSM is now enabled, and the Delinea Secret Server encryption key is stored on it. The nShield Connect HSM configuration details appear on the Delinea Secret Server **HSM** tab.

Secret Server	× +							-		×
\leftarrow \rightarrow G (2)	O 🗅 localhost/Secre	O D localhost/SecretServer/ConfigurationHsm.aspx			Ē	80%	☆		\bigtriangledown	≡
thycotic,								Q	0	4
G Home	Configuration									
(S) Recent										
O Shared With Me	General Login SAML	Folders Local User Passwords	Security Ticket System	Email Session Re	ecording	HSM				
☆ Favorites	Enable HSM		Yes							
Ļ Inbox	Persistent Provider	Persistent Provider nCipher Security World Key Storage Provider								
Reports +	Key Identifier									
🔓 Secrets +	Key Size 4096-bit Key Update Completed Date 3/10/2022 11:37 AM									
	Sack Disable HSN	1 13 Rotate HSM Key	View Audit							
د Admin د										

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

1. Copy the cryptoki library file

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

to C:\inetpub\wwwroot\SecretServer\pkcs11

so that Delinea Secret Server can see it.

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

Secret Server	× +				- 0	×
← → C = delinea2.in	terop.local/SecretServer/ConfigurationHsm.asp	х		\$:
Secret Server					Q	0
Dashboard	Configuration					
A Secrets	General Login SAML Folders	Local User Passwords Security	Ticket System Email Ses	sion Recording HSM		
Û Inbox	We recommend enabling with	the new PKCS11 API Type using an AE	S 256 key. This is only available i	n the New UI. Click here to a	enable with	
Reports	PKCS11 options.					
Administration	Enable HSM		No			
	Sack Tenable HSM	View Audit				

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

Configuration - Secret Server	× +						- 0	×
← → C : delinea2.interop.local/SecretServer/app/#/admin/configuration/hsm 🗠 🛠						:		
Secret Server	Admin > Configuration Overview >			Q (?)	÷	Û (5 🗉	S
Dashboard	Configuration							
Secrets	Enable HSM This allows you to integrate with hardware	security modules (HSMs). When configured to	o use an HSM, the encryption	ı				
II Reports	key and the Secret keys are protected by that HSM. HSM Integration Guide &							
Administration >>	API Type *	PKCS11				~]	
	Library Name *	cknfast.dll				~		
	Token Label *	secretserverocs]	
	User Pin *	•••••				0]	
	Кеу Туре *	AES				~]	
	Key Size *	256				~]	
				Cano	el	Next		

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



6. Verify the HSM configuration, then select Next



3.3. Verify integration

Verify the keys generated by the Delinea Secret Server are stored in the nShield HSM.

Run the nfkmverify utility.

```
C:\Users\Administrator>nfkmverify
** [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
```

14/15

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 4. Additional resources and related products

- 4.1. nShield Connect
- 4.2. nShield as a Service
- 4.3. Entrust products
- 4.4. nShield product documentation