



Delinea Secret Server

nShield[®] HSM Integration Guide

2025-07-02

© 2025 Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction
1.1. Product configurations
1.2. Supported nShield hardware and software versions
1.3. Supported nShield features
1.4. Requirements
2. Deploy and configure the Delinea Secret server
3. Deploy and configure the nShield HSM
3.1. Install the Entrust nShield HSM
3.2. Install the Security World software and create a Security World
3.3. Select the protection method
3.4. Create the OCS
3.5. Create the softcard
3.6. Automatically start the nShield service agent at startup
4. Integrate Delinea Secret Server with an Entrust nShield HSM
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
4.3. Verify integration
5. Additional resources and related products
5.1. nShield Connect
5.2. nShield as a Service
5.3. Entrust products
5.4. nShield product documentation

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	11.8.000001
SQL Server 2022	16.0.1000 Express Edition
SQL Server Management Studio 21	21.1.3
IIS	10.0.20348.1
Base OS	Microsoft Windows Server 2022

1.2. Supported nShield hardware and software versions

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

HSM	Security World Software	Firmware	Netimage
Connect 5c	13.6.11	13.4.5 (FIPS 140-3 certified)	13.6.11
nShield XC	13.6.11	12.72.3 (FIPS 140-2 certified)	13.6.7

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			

Feature	CNG Cryptography Provider	PKCS #11 API
Module Only Key	Yes	Yes
Operator Card Set (OCS)	Yes but without a passphrase	Yes
nSaaS	Supported but not tested	Supported but not tested

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

The Secret Server was deployed on a domain joined Windows virtual machine. Microsoft IIS was installed on the virtual machine, and bound to the virtual machine certificate. The Secret Server connected to an existing Microsoft SQL database. This database was also installed on the same virtual machine. A domain managed service account was created for the above connections. All permissions where set according to Delinea Documentation - Secret Server Setup.



Chapter 3. Deploy and configure the nShield HSM

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

3.1. Install the Entrust nShield HSM

Install the nShield Connect HSM locally, remotely, or remotely via the serial console. Condensed instructions are available in the following Entrust nShield Support articles.

- How To: Locally Set up a new or replacement nShield Connect.
- · How To: Remotely Setup a new or replacement nShield Connect.
- How To: Remotely Setup a new or replacement nShield Connect XC Serial Console Model.

For detailed instructions see the nShield v13.6.11 Hardware Install and Setup. Guides.

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

- 1. Install the Security World software. For detailed instructions see the nShield Security World Software v13.6.11 Installation Guide.
- 2. Add the Security World utilities path to the system path. This path is typically C:\Program Files\nCipher\nfast\bin.
- 3. Open the firewall port 9004 for the HSM connections.
- 4. If you are using remote administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).
- 5. Inform the HSM of the location of this client computer as described Configuring the nShield HSM to use the client.
- 6. Configure this client to use the HSM as described Configuring client computers to use the nShield HSM.
- 7. Open a command window and run the following utility to confirm that the HSM is **operational**:

```
C:\Users\Administrator.INTEROP>enquiry
Server:
enquiry reply flags none
enquiry reply level Six
serial number xxxx-xxxx xxxx-xxxx xxxx-xxxx
mode operational
```

version	13.6.11
Module #1:	
enquiry reply flags	UnprivOnly
enquiry reply level	Six
serial number	XXXX-XXXX-XXXX
mode	operational
version	13.4.5
Module #2:	
enquiry reply flags	UnprivOnly
enquiry reply level	Six
serial number	XXXX-XXXX-XXXX
mode	operational
version	12.72.3

 Create your 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.

9. Confirm that the Security World is "Usable*:

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

3.3. Select the protection method

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

- Operator Cards Set (OCS) are 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 softcards use, see Softcards.

• Module protected keys are simply protected by a module key. For more information on module protection use 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 and card set state
NFAST_NFKM_TOKENSFILE="C:\Program Files\nCipher\nfast\preloadtoken"
```

3.4. Create the OCS

CKNFAST_NONREMOVABLE=1

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></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
FIPS 140-2 level 3 auth obtained.
Creating Cardset:
Module 1: 0 cards of 1 written
Module 1 slot 0: Admin Card #1
Module 1 slot 2: empty
Module 1 slot 2: blank cardSteps:
Module 1 slot 2: blank cardSteps:
Card writing complete.
cardset created; hkltu = 7aaf758bc6790206198ea5218040d4faa09f035f
```

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

1 testOCSnopassphrase

2 testOCS

1 (1)

1 of 5

rocs> exit
```

3.5. 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
Enter new pass phrase:
Enter new pass phrase again:
New softcard created: HKLTU d23456789234567234567471d3722f8c70f5d864
```

4. Verify the softcard.

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> guit
```

3.6. 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

- 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 Install the Security World software and 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.

Х

Example for OCS protection:

nShield CNG Providers Configuration Wizard

Current Operator Card Sets:	Operator Card Set Tok	ken Information:	
testOCSnopassphrase	Name: Token hash: Sharing parameters:	testOCSnopassphrase 0x7aaf758b 1 of 5. Non-persistent	
	Timeout:	None	
	Currently protecting:	none	
Create a new Operator Card Set	name		
Number of cards required (K):	Tota	al number of cards (N):	
Card set has a time-	out Card set time-	out: seconds	
Persistent	Usable remotely		

6. Run certutil -csptest > <filename> on a command window.

For example:

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

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

🧾 cryptographic-providers - Notepad			
File Edit Format View Help			
Provider Name: nCipher Security World Key Sto Name: nCipher Security World Key Storage Pr HWND Handle:Binary: 0000 00 00 00 00 00 00 00 Impl Type: 17 (0x11) NCRYPT_IMPL_HARDWARE_FLAG 1 NCRYPT_IMPL_HARDWARE_RNG_FLAG 10 (16)	brage Provider rovider 		
Version: 851974 (0xd0006) <mark>Pass</mark>	Find		×
Dravidan Madula:	Find what: Provider Name: n	Cipher	Find Next
UM(1): nckspsw.dll		Direction	Cancel
0(1): 10001, 0 0: KEY_STORAGE	Match case	⊖ Up ● Down	
-	Wrap around		
Asymmetric Encryption Algorithms: RSA			
BCRYPT_ASYMMETRIC_ENCRYPTION_INTERFACE NCRYPT_ASYMMETRIC_ENCRYPTION_OPERATION NCRYPT_SIGNATURE_OPERATION 10 (16)	- 3 - 4		
Secret Agreement Algorithms:			
<			
Found next from the top		Ln 3395, Col 3	100% V

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



- 10. Select Enable HSM. Then select Next.
- 11. In the Enable HSM window, select as follows. Then select Next.

Parameter	Value
API type	CNG
Persistent provider	nCipher Security World Key Storage Provider
Key type	RSA
Key size	Your selection
Padding type	OAEP (PKCS1 is not supported)

For example:

🕖 HSM - Se	cret Server × +			\sim	- 🗆 X
$\leftarrow \ \ \rightarrow \ \ G$	http://localhost/S	ecretServer/app/#/admin/co	onfiguration/hsm	\$	@ ☆ ≡
	Settings All settings Configuration search	Settings > Configuration	n search > Q (? ⊕ 1	¥ 🖪 🕛
Secrets	Distributed Engine Sites and engines	This allows you to integ configured to use an HS by that HSM.	rate with hardware secu SM, the encryption key a	irity modules (H nd the Secret k	SMs). When eys are protected
Discovery	Site connectors Configuration Log	API type *	CNG		~
Access	Audit	Persistent provider * Key type *	nCipher Security World	l Key Storage Pro	vider ~
	SSH	Key size *	4096		~
کیک Settings	RDP SSH terminal	 Selecting a key size will significantly im 	larger than 2048-bit wi pact performance.	ill increase sec	urity, however
	Endpoint configuration	Padding type *	OAEP		~
«	Remote password changing Configuration			Cance	Next
HSM	∧ ∨ □ Highlig	ght <u>A</u> ll 📃 Match <u>C</u> ase 📃 I	Match D <u>i</u> acritics <u>W</u> ho	le Words 1 of	I match X

12. Check the HSM Provider Test Results. Then select Next.



13. In the Verify HSM configuration page select Save.



14. In the **Notice** about HSM configuration change, recycle the application pool. Then select **Continue**.

💐 Internet Information Services (IIS) Manager						- 🗆 X
← → @ ► DELINEASECRETSR ► Applicat	tion Pools					🔯 🖂 🟠 🔞 -
File View Help						
Connections					Ac	tions
Image: Start Page Image	TEROP\Administrator) TEROP\Administrator) Tere fitter: Tere filter: Te					Add Application Pool Set Application Pool Defaults Application Pool Tasks Start
 Oefault Web Site aspnet_client 					2	Stop Recycle
> P SecretServer	Name	Status	.NET CLR V	Manage ^		Edit Application Pool
> TMS	.NET v2.0 Classic	Started	v2.0	Classic		Basic Settings
	.NET v4.5	Started	v4.0	Integrat		Recycling
	.NET v4.5 Classic	Started	v4.0	Classic		Advanced Settings
	Classic .NET Ap	Started	v2.0	Classic		Rename
	DefaultAppPool	Started	v4.0	Integrat	×	Remove
	SecretServer	Started	v4.0	Integrat		View Applications
	Features View	Content Vie	v4.0	>	0	Help
Ready						¶ <u>∎</u> .:

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

💿 HSM - Se	cret Server × +			\sim	- 🗆 X
$\leftarrow \ \ \rightarrow \ \ C$	http://localhost/	SecretServer/app/#/admin/o	configuration/hsm	☆	€ 1 €
G Home	Settings All settings Configuration search	Settings > Configurati	on search > Q Enable HSM Di	⑦ ⊕ sable HSM	Rotate HSM key
Secrets	Distributed Engine Sites and engines Site connectors	HSM configura This allows you to inte configured to use an H by that HSM.	tion grate with hardware se ISM, the encryption ke	ecurity modules y and the Secre	(HSMs). When t keys are protected
II Reports	Configuration Log Audit	HSM integration guid Enable HSM API type	e ௴ Yes CNG		
Access CD Inbox	Proxying SSH	Persistent provider Key identifier Key type	nCipher Security Wo RSA	rld Key Storage	Provider
کیک Settings	RDP SSH terminal	Key size Padding type	4096 OAEP		
«	Endpoint configuration Remote password changing Configuration	Key Update Completed Date	672672025 01:34 PM		
HSM	∧ ∨ □ Highli	ight <u>A</u> ll Match <u>C</u> ase	Match Diacritics	Vhole Words 1	of 1 match Reacher 🗙

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.

- If the HSM was previously configured using the CNG cryptography provider, select Disable HSM, recycle the application pool, and refresh the browser. Otherwise, continue to the next step.
- 3. Copy the HSM cryptoki library (dll) for PKCS #11 to the Secret Sever application pool as shown:

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

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



- 6. Select Enable HSM. Then select Next.
- 7. In the Enable HSM window, select as follows. Then select Next.

Parameter	Value
API type	PKCS11
Library name	cknfast.dll
Token label	<ocs cardset="" name=""></ocs>
User pin	<ocs cardset="" passphrase=""></ocs>
Key type	AES

Parameter	Value
Key size	256

For example:

🚺 HSM - Se	cret Server × +			\sim	- 🗆 X				
$\leftarrow \ \ \rightarrow \ \ {\tt C}$	http://localhost/S	ecretServer/app/#/admin/c	onfiguration/hsm	\$: එ ≡				
G Home	Settings All settings Configuration search	Settings > Configuration	on search > Q	୭ ⊕ 4					
Secrets	Distributed Engine Sites and engines	This allows you to integ configured to use an H by that HSM.	grate with hardware securi SM, the encryption key an	ity modules (HS d the Secret ke	Ms). When ys are protected				
Ø Discovery	Site connectors	HSM integration guide 앱							
al	Configuration	API type *	PKCS11		~				
Reports	Audit	Library name *	cknfast.dll		~				
Access	Proxying	Token label *	testOCS						
Inbox	SSH	User pin *	• • • • • • •		۲				
63	RDP	Key type *	AES		~				
Settings	SSH terminal Endpoint configuration	Key size *	256		~				
«	Remote password changing Configuration			Cancel	Next				
HSM	∧ ∨ □ Highlig	ht <u>A</u> ll Match <u>C</u> ase	Match Diacritics Whole	Words 1 of 1	match Reacher 🗙				

8. Check the HSM Provider Test Results. Then select Next.



9. In the Verify HSM configuration page select Save.

🚺 HSM - Se	cret Server × +			\sim	– 🗆 X
$\leftarrow \rightarrow C$	http://localhost/Superior	ecretServer/app/#/admi	n/configuration/hsm	☆	: එ =
Home Secrets	Settings All settings Configuration search Distributed Engine Sites and engines Site connectors	Settings > Configure Verify HSM ccc Please review your H 1. The encryptin 2. The database 3. You will peed	ation search > Q onfiguration HSM configuration. Contin on.config file will be modified will be updated with the to recycle the application		K II I
Discovery I Reports Access	Configuration Log Audit	API type Library name Token label User pin	PKCS11 cknfast.dll testOCS ******* Show		
Inbox	Proxying SSH	Key type Key size	AES 256		
Settings	RDP SSH terminal Endpoint configuration Remote password changing			Can	Cel Save
HSM	Configuration	ht <u>A</u> ll Match <u>C</u> ase [Match Diacritics	<u>/</u> hole Words 1 of	1 match Reacher 🗙

10. In the **Notice** about HSM configuration change, recycle the application pool. Then select **Continue**.

Internet Information Services (IIS) Manager						- 🗆 X			
C DELINEASECRETSR + Application Pools						😰 🖂 🚱 -			
File View Help									
Connections						Actions			
Image: Start Page Image: DELINEASECRETSR (INTEROP\Administrator) Image: Delinease of the start of the	Application POOIS This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.					Add Application Pool Set Application Pool Defaults Application Pool Tasks Start			
 Oefault Web Site i aspnet_client 	Filter: • 🐨 Go - 🖓 Show All			2	Stop Recycle				
> P SecretServer	Name	Status	.NET CLR V	Manage ^		Edit Application Pool			
> 😭 TMS	.NET v2.0 Classic	Started	v2.0	Classic		Basic Settings			
	.NET v4.5	Started	v4.0	Integrat		Recycling			
	.NET v4.5 Classic	Started	v4.0	Classic		Advanced Settings			
	Classic .NET Ap	Started	v2.0	Classic		Rename			
	DefaultAppPool	Started	v4.0	Integrat	×	Remove			
	SecretServer	Started	v4.0	Integrat		View Applications			
	Eestures View	Content Vie	V4.U	>	0	Help			
Ready		Jontent vie	vv			• <u>.</u>			

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

🔘 HSM - Se	ecret Server × +			\sim	1	-		\times		
$\leftarrow \ \ \rightarrow \ \ C$	http://localhost/S	ecretServer/app/#/admin/	configuration/hsm		\$	۲	ර	≡		
₽	Settings	Settings > Configurat	ion search > C	2 ?	⊕ €					
Home	Configuration search	nomconngaration								
0	Distributed Engine Sites and engines	This allows you to integrate with hardware security modules (HSMs). When configured to use an HSM, the encryption key and the Secret keys are protected by the HSM.								
Secrets		HSM integration guide 🕫								
Discovery	Site connectors	Enable HSM	Yes					- 1		
al	Configuration	API type	PKCS11							
Reports	Log	Library name	cknfast.dll							
ද	Audit	Token label	testOCS							
Access	Proxying	User pin	rrpin ********⊗							
	SSH	Key identifier	Sector description							
Inbox		Key type	AES							
(ý)	RDP	Key size	256							
Settings	SSH terminal									
	Endpoint configuration	Secret Key Update Progress	Enabling mainten shortly.	nance mode. F	Processing	will beg	in			
«	Remote password changing									
HSM		abt All Match Case	Match Diagritics	Whole Wor	ds 1 of 1 -	match	Reacho	X		
		nic En En march Ease	materiojacines		10111	naturi	neucile	\sim		

4.3. Verify integration

1. List the keys protected by the HSM using the nfkminfo utility.

C:\Users\Administrator.INTEROP>nfkminfo -1

```
Keys protected by cardsets:
key_pkcs11_ucedb3d45a28e5a6b22b033684ce589d9e198272c2-5c65ec9a8fd17ea4ff069e88f552f926d35252d0 `5a7ea9ae-
d562-40c5-9091-25f76d55b529'
```

2. Notice the **Key identifier** in the completed HSM configuration matches the nfkminfo utility output above. In this case the key corresponds to the the Delinea Secret Server using the PKCS #11 API.

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 Connect
- 5.2. nShield as a Service
- 5.3. Entrust products
- 5.4. nShield product documentation