

Member of Microsoft Intelligent Security Association

Microsoft Security

# Microsoft Host Guardian Service and Shielded Virtual Machines

nShield<sup>®</sup> HSM Integration Guide 2023-12-05

© 2023 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
1.5. More information
2. Procedures
2.1. Install and configure the nShield Security World software and nShield
HSM
2.2. Install and register the nShield CNG
2.3. Install the Host Guardian Service in a new forest
2.4. Generate certificates
2.5. Initialize the Host Guardian Service
2.6. Configure the Guarded Host
2.7. Configure attestation on the Guardian Server
2.8. Configure attestation on the Guarded Host
3. Troubleshooting
4. Remote Administration

# Chapter 1. Introduction

The Entrust nShield HSMs secure keys that encrypt and sign the protected VMs. The keys are stored in an encrypted state on the Host Guardian Server (HGS).

The Guarded Host provides a trusted server and environment in which to create and run the Shielded VMs. The HGS attests the trustworthiness of a particular Guarded Host before releasing the relevant protection key used to unlock (decrypt), the virtual machine.

The HGS only releases the decryption key for the Shielded VM when it is satisfied that the condition of the VM matches a known clean state and that the VM has not been tampered with. This is achieved by providing evidence to attest to the VM's integrity via a certificate that is also provided by the HGS.

Attestation process for running Shielded VMs on a Hyper-V Guarded Host:

- 1. The Guarded Host requests a key to allow it to run the Shielded VM.
- 2. The HGS receives the request but does not trust that the request comes from a legitimate host.
- 3. The Guarded Host sends its declaration of health information, a known state conferred upon the host by the HGS in the initial set-up of the Hyper-V host.
- 4. The HGS responds with a certificate of health to the host.
- 5. The host makes another request, which includes the certificate to the HGS.
- 6. The HGS returns the encrypted key to the virtualized security area of the Guarded Host, allowing the VM to run.

# 1.1. Product configurations

Entrust has successfully tested nShield HSM integration with Windows Hyper-V feature in the following configurations:

Product	Version
Guardian Server Base OS	Windows Server 2019 Datacenter
Guarded Host Base OS	Windows Server 2019 Datacenter

# 1.2. Supported nShield features

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

Feature	Support
Operator Card Set (OCS)	Yes
Softcard Protection	Yes
Module	Yes

# 1.3. Supported nShield hardware and software versions

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

Product	Security World Software	Firmware	Image	OCS	Softcard	Module
Connect +	12.80.4	12.50.8 (FIPS Certified)	12.80.4	$\checkmark$	$\checkmark$	$\checkmark$
Connect XC	12.80.4	12.50.11 (FIPS Certified)	12.80.4	$\checkmark$	$\checkmark$	$\checkmark$
Connect XC	12.80.4	12.72.1 (FIPS Certified)	12.80.5	$\checkmark$	$\checkmark$	$\checkmark$
nShield 5c	13.2.2	13.2.2 (FIPS Pending)	13.2.2	$\checkmark$	$\checkmark$	$\checkmark$

## 1.4. Requirements

Familiarize yourself with the Microsoft Hyper-V and Guarded Hosts documentation and set-up process.

Before installing these products, read the associated nShield HSM Installation

#### Guide and User Guide.

This guide assumes familiarity with the following:

- 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. The OCS can also provide key protection for the Vault master key. For information about limitations on FIPS authorization, see the *Installation Guide* of the nShield HSM.



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

- Whether to instantiate the Security World as recoverable or not.
- Network environment set-up, via correct firewall configuration with usable ports: 9004 for the HSM and 9005 for remote administration.

## 1.5. More information

For more information contact your 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

The following steps summarize the integration procedure.

Guardian Server:

- 1. Install and configure the nShield Security World software and nShield HSM.
- 2. Install and register the nShield CNG.
- 3. Install the Host Guardian Service in a new forest.
- 4. Generate certificates.
- 5. Initialize the Host Guardian Service.

#### Guarded Host:

- 1. Configure the Guarded Host.
- 2. Configure attestation on the Guardian Server.
- 3. Configure attestation on the Guarded Host.



For this guide both the Guardian Server and Guarded Host were implemented on virtual machines. Microsoft recommends installing the Host Guardian Service role on a physical machine for security purposes.



The Host Guardian Service should be installed in a dedicated Active Directory forest. Ensure the Guardian Server and Guarded Host are not joined to a domain.

# 2.1. Install and configure the nShield Security World software and nShield HSM

1. Install the Security World software on the Guardian Server:

- a. Mount the DVD or .iso disc image.
- b. Run setup.exe.
- c. Right-click the icon and select **Run as Administrator**.

For detailed instructions, see the *Installation Guide* and the *User Guide* for the HSM.

N   → File Hom	e Share View Manage	DVD Drive (D:) nCipher Security World		- □ × ~ ?
$\leftarrow$ $\rightarrow$ $\cdot$ $\prime$	↑ Ň > Computer Name: LT > [	OVD Drive (D:) nCipher Security World	✓ ບ Search DVD Dri	ve (D:) nCipher 🔎
▶ ^	Name	Date modified	Туре	Size ^
> 📜	documentation	6/25/2020 1:06 AM	File folder	
> 📜	📜 license	6/25/2020 1:06 AM	File folder	
> 📜	📕 release	6/25/2020 1:06 AM	File folder	
<b>1</b> - 1	🚮 autorun	6/25/2020 1:06 AM	Setup Information	1 KB
<b>1</b>	🗾 nCipher-EULA	6/25/2020 1:06 AM	Adobe Acrobat Docu	210 KB
> 📜 📃	N nCipher-N	6/25/2020 1:06 AM	lcon	104 KB
	👘 setup	6/25/2020 1:06 AM	Windows Installer Pa	588,956 KB
· · ·	version	6/25/2020 1:06 AM	Text Document	1 KB 🗸
8 items				E 1

- 2. Add the Security World utilities path C:\Program Files\nCipher\nfast\bin to the Windows system path.
- 3. Open the firewall port 9004 for the HSM connections.
- 4. 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.

5. Open a command window and run the following to confirm that the HSM is **operational**:

>enquiry Server: enquiry reply flags enquiry reply level serial number mode	none Six 530E-02E0-D947 7724-8509-81E3 09AF-0BE9-53AA 9E10-03E0-D947 operational
 Module #1: enquiry reply flags enquiry reply level serial number mode	none Six 530E-02E0-D947 operational

6. Create your Security World if one does not already exist or copy an existing one. Follow your organization's security policy for this. The Security World can also be created later, when configuring the CNG provider via its GUI, see Install and register the nShield CNG. Skip the next step if doing so. 7. Confirm that the Security World is **usable**:

```
>nfkminfo
World
generation 2
state 0x37270008 Initialised Usable ...
...
Module #1
generation 2
state 0x2 Usable
...
```

### 2.2. Install and register the nShield CNG

It is necessary to install and register the nShield Cryptography API: Next Generation (CNG) provider on the Guardian Server. This can be done using either the command line or the **CNG Configuration** wizard.

Before proceeding, check that no legacy providers are installed.

1. Run the command:

```
>cnglist.exe --list-providers
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation.
All rights reserved.
C:\Users\Administrator>cd %nfast_home%\bin
C:\Program Files (x86)\nCipher\nfast\bin>cnglist.exe --list-providers
Microsoft Key Protection Provider
Microsoft Platform Crypto Provider
Microsoft Platform Crypto Provider
Microsoft Smart Card Key Storage Provider
Microsoft Software Key Storage Provider
Microsoft SSL Protocol Provider
Windows Client Key Protection Provider
C:\Program Files (x86)\nCipher\nfast\bin>
```

- 2. Select the **Start** button to access all applications. Look for the recently installed nShield utilities.
- 3. Double-click the CNG Configuration wizard and run it as Administrator.



#### The nShield CNG Providers Configuration Wizard starts.

nShield CNG Providers Config	juration Wizard	$\times$
ENTRUST	Welcome to the nShield support software Cryptographic Service Providers. NShield CNG Providers enable the use of nShield modules with the wide range of security-enabled applications provided with Windows. If you have not already created an nShield security world or a suitable card set, the wizard guides you through their creation before registering the CNG Providers. To continue, click Next.	
	< Back Next > Cance	el

4. On the Welcome panel, select Next.

The **Enable HSM Pool Mode** panel appears.



5. If you intend to use multiple HSMs in a failover and load-sharing capacity, select **Enable HSM Pool Mode for CNG Providers**. If you do, you can only use

module protected keys.



Module protection does not provide conventional 1 or 2 factor authentication. Instead, the keys are encrypted and stored as an application key token, also referred to as a Binary Large Object (blob), in the kmdata/local directory of the HGS server.

6. Select Next.

The Initial setup panel appears:

nShield CNG Providers Configuration Wizard	×
Initial setup Perform initial setup steps required by nShield Windows Support Software.	
You already have a security world set up on this server. You can use this security w or create a new security world.	orld
Use the existing security world	
Select this option to keep all your existing settings and keys, allowing you to integrate new nShield modules into an existing security world.	
Create a new security world	
Select this option to create a totally new security world; all your existing card sets private keys, and certificates created with the nShield modules will stop working, existing security world is backed up. Only select this option if you do not have an existing security world or are sure you need a new security world environment.	s, Any I
< Back Next >	Cancel

- Select Use the existing security world if you already have a Security World that you intend to use. The corresponding world and module\_xxxxxxxx-xxxx files must be present in the %NFAST\_KMDATA%\local directory. Be prepared to present the quorum of Administrator cards.
- Select Create a new Security World if you do not currently have a Security World or would like to create a new Security World.



For the purposes of this guide, an existing Security World is used. For instructions on how to create and configure a new Security World, see the *Installation Guide* and *User Guide* for your HSM.

7. Select Next.

The Set Module States panel appears.

Ensure modul	es are in the correct s	state before you proceed.	
The following	modules are available	e in your system:	
Module ID	Mode	State	
1	operational	usable	
2	operational	foreign	
At least one n Or reset modu uninitialized n	nodule is usable in the ile 2 to the initializatio Shield modules.	e current world. Click Next to continu n state to enable you to restore your	e with this wor security world

- 8. Select the desired HSM among those available.
- 9. Select Next.

#### The Key Protection Setup panel appears.

nShield CNG Providers Configuration Wizard	×
Key Protection Setup Set up the private key-protection method.	ENTRUST
Select the default method that will be used to protect private keys generated by the CNG Key Storage Provider.	
If softcard or OCS protection is selected, the choice will be offered on the next page whether to use an existing token or create a new one.	
O Module protection (requires no extra cards but is less secure).	
O Softcard protection (unavailable in HSM Pool Mode).	
Operator Card Set protection (unavailable in HSM Pool Mode).	
○ Allow any protection method to be selected in the GUI when generating.	
< Back Next > C	ancel

10. Select the required protection method.

For the purposes of this guide, **Operator Card Set** is used. You can choose **Module Protection** or **Softcard Protection** instead.

#### 11. Select **Next**.

The Token for Key Protection panel appears.

Shield CNG Providers Configuration Token for Key Protection Select the token that will be use	on Wizard d to protee	ct new keys, or create a new token.
Current Operator Card Sets:	Opera	ator Card Set Token Information:
No tokens found.	Nam	e:
	Tok	en hash:
	Shar Time	ing parameters:
	- Time Cum	entu protecting
	Can	sity protocing.
🗹 Create a new Operator Card S	et name	MSAuthenticode
Number of cards required (K	(): <b>1</b>	Total number of cards (N): 1
Card set has a tim	ie-out	Card set time-out: seconds
Persistent	🗹 Usabl	e remotely
		< Back Next > Cancel

- 12. Enter the OCS name, K and N values, select **Persistent**, and select **Usable remotely**.
- 13. Select Next.

You must now present the cards.

14. First present the ACS to the HSM.

Then remove the ACS and insert a blank Operator Card in the HSM. On the **Insert Next Card** screen enter a name for the OCS and corresponding passphrase.

nShield CNG Providers Configuration Wizard	$\times$
Insert Next Card Insert the next card in the sequence.	
Preparing to write Operator Card number 1 of 1. Insert a blank card in module 1. Name of card: MSAuthenticode	
Card requires a pass phrase	
Enter pass phrase:	
Re-enter pass phrase:	
Enter and repeat the pass phrase for this card, and then click Next to write inform to the card.	nation
< Back Next >	Cancel

- 15. Select **Next** and repeat until all cards in the OCS have been presented.
- 16. Select Finish.

The nShield CNG providers will now be installed and the Key Storage Provider will be registered.

C-B		
Ready to install nShield support software.		
		ENTR
You now have a valid security world and now register the nShield CNG Providers. T providers, and you must select them explic press Next to continue.	key protection mechanisr [he nShield providers will sitly by name through you	n. The Wizard will not be default ir application. Please

After this process completes, the **Finished Registering the nShield CNG Providers** panel appears.

nShield CNG Providers Config	guration Wizard	$\times$
	Finished registering the nShield CNG Providers	
	nShield CSPs are installed and your security world is ready for use.	
ENTRUST		
	< Back Finish Cance	4

17. Open a command window as Administrator and run the following command to confirm the KSP has been successfully registered:

> cnglist.exe --list-providers Microsoft Key Protection Provider Microsoft Passport Key Storage Provider Microsoft Platform Crypto Provider Microsoft Primitive Provider Microsoft Smart Card Key Storage Provider Microsoft Software Key Storage Provider Microsoft SSL Protocol Provider Windows Client Key Protection Provider nCipher Primitive Provider nCipher Security World Key Storage Provider

Look for the nCipher Security World Key Storage Provider entry.

18. Run the following from PowerShell after the Host Guardian Service has been installed:

Show-DnsServerKeyStorageProvider Microsoft Software Key Storage Provider nCipher Security World Key Storage Provider Microsoft Passport Key Storage Provider Microsoft Platform Crypto Provider Microsoft Smart Card Key Storage Provider

 Check that the registry also shows the nCipher Security World Key Storage Provider:

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Cryptography\Providers\nCipherSecurityWorldKeyStorageProvid er

For example:



## 2.3. Install the Host Guardian Service in a new forest

This section describes how to install the Host Guardian Service in a new Active Directory forest:

- Add the Host Guardian Server role using the Server Manager GUI.
- Add the Host Guardian Server role using PowerShell.
- Install the Host Guardian Service.

Microsoft has documented the full process in https://technet.microsoft.com/enus/windows-server-docs/security/guarded-fabric-shielded-vm/guarded-fabricdeploying-hgs-overview.

#### 2.3.1. Add the Host Guardian Server role using the Server Manager GUI



You can also add the Host Guardian Server role using

PowerShell, see Add the Host Guardian Server role using PowerShell.

To add the Host Guardian Server using the Server Manager GUI:



1. Open Server Manager and under Manage, select Add Roles and features.

The Add Roles and Features Wizard starts.

- 2. Select Next until you reach the Select destination server panel.
- 3. On the **Select destination server** panel, select the Guardian Server. For example:

Land Roles and Features Wizard	I			-		×
Select destination	n server			DESTINA Hos	FION SER\ tGuardian	/ER iSrv
Before You Begin Installation Type Server Selection	Select a server or a virt Select a server from Select a virtual hard	tual hard disk on which n the server pool d disk	to install roles and features.			
Server Roles	Server Pool					
Features	511.					_
	Filter:					
	Name	IP Address	Operating System			
	HostGuardianSrv	10.194.148.79	Microsoft Windows Server 20	19 Datacenter		
	1 Computer(s) found This page shows serve and that have been ad newly-added servers fi	rs that are running Wind Ided by using the Add S rom which data collectic	dows Server 2012 or a newer rek ervers command in Server Mana n is still incomplete are not shor	ease of Windo Iger. Offline se wn.	ws Serve rvers an	er, d
		< Pre	vious Next >	Install	Cance	ł

4. Select Next.

The Select server roles panel appears.

5. Select Host Guardian Service.

The **Add features that are required for Host Guardian Service?** dialog appears.

elect server ro	les	Add Roles and Features Wizard
Before You Begin Installation Type	Select one or more ro	Add features that are required for Host Guardian Service?
Server Roles Server Roles Features Confirmation Results	Active Direct Active Direct Active Direct Active Direct Control Direct Device Healt DHCP Server DKS Server E File and Store Hyper-V Network Cont Print and Do Remote Desk Volume Activ Web Server ( Windows De	Vou cannot install Host Guardian Service unless the following role services or features are also installed.

- 6. In the dialog, select Add Features and select Next.
- 7. Select **Next** multiple times until the install for the **Select role services** panel for Web Server Role (IIS) appears.

Installation Type     Role services     Description       Server Selection     ✓ MebServer     WebServer provides support       Features     ✓ Common HTTP Features     WebServer provides support       AD DS     ✓ Directory Browsing     ✓ Sever to host an inter- external Web Server to host an inter- graphic Contern Logging Diging Tools DOBE Logging Security     Features       Confirmation Prannic Content Compression Security     ✓ Heroting	elect role servi Before You Begin	2S DESTINATION SERVER HostGuardianSrv Select the role services to install for Web Server (IIS)
< >>	Installation Type Server Roles Features AD DS Host Guardian Service Web Server Role (IIS) Role Services Confirmation Results	Old services       Description         Image: Service Servi

8. Select Next to install IIS and then select Install.

After the installation completes, a server restart is required.

After the role has been added, you are prompted to continue with **Postdeployment Configuration** by promoting the server to a domain controller. This is shown by expanding the notification flag in the **Server Manager Dashboard**.



Do not promote to domain controller at this time. The server will be promoted as part of the HGS installation process below.

Server Manager		- 🗆 X
(€) → ··· Dash	board	🕶 🕝   🍢 Manage Tools View Help
Dashboard     Local Server     All Servers     All Servers     AD DS     File and Storage Service:	Post-deploy Configuratic Services at I Promote thi Task Details	ent Configura TASKS V   X required for Active Directory Domain SSTGUARDIANSRV server to a domain controller this local server
Host Guardian Service     To IIS	WHAT'S LEARN I	2 Add roles and features 3 Add other servers to manage 4 Create a server group 5 Connect this server to cloud servic Hide
	ROLES A	VD SERVER GROUPS Server groups: 1   Servers total: 1

### 2.3.2. Add the Host Guardian Server role using PowerShell



You can also add the Host Guardian Server role using the Server Manager GUI, see Add the Host Guardian Server role using the Server Manager GUI.

To add the Host Guardian Server role using PowerShell:

- 1. Start PowerShell in an elevated Admin mode.
- 2. Run the following command:

Install-WindowsFeature -Name HostGuardianServiceRole -IncludeAllSubFeature -IncludeManagementTools -Restart



Do not promote to domain controller at this time. The server will be promoted as part of the HGS installation process below.

#### 2.3.3. Install the Host Guardian Service

To install the Host Guardian Service:

- 1. Launch PowerShell as Administrator.
- 2. Run the Install\_HGS.ps1 script (below) to install the Host Guardian Service and configure its domain.

```
$hgsDomainName = "hgs.com"
$adminPassword = ConvertTo-SecureString -AsPlainText "xxxxxxxxxx" -Force
Install-HgsServer -HgsDomainName $hgsDomainName -SafeModeAdministratorPassword $adminPassword -Restart
```

The password you specify here will only apply to the Directory Services Repair Mode password for Active Directory. It will not change your admin account's password.

You may provide any domain name of your choosing for -HgsDomainName.

The server will reboot after executing the above script.

The Host Guardian Service domain is created.



### 2.4. Generate certificates

The following sections describe how to generate certificates:

- 1. Generate certificates using the nShield key storage provider.
- 2. Confirm certificates and keys.

# 2.4.1. Generate certificates using the nShield key storage provider

The HGS requires certificates and associated keys.

Keys are used for "attestation", one of the two services that run as part of HGS, to affirm the health of the Guarded Hosts and the associated Hyper-V virtual machines.

Other keys called Transport Keys (TKs) are used for "Key Protection Service" (KPS), to unlock and run the Shielded VMs on positively attested Guarded Hosts.

Run **certutil** -**store** my for the certificates currently available in the machine store. For example:

```
>certutil -store my
my "Personal"
CertUtil: -store command completed successfully.
```



It is possible to use conventionally backed Certificates from a Certificate Authority and import these into the HSM Security World, but this is not within the scope of this document.

The following sections generate these keys and certificates using the nShield KSP.

#### 2.4.1.1. Generate encryption certificate

To generate an encryption certificate:

- 1. Launch PowerShell as Administrator.
- 2. Run the following script: Generate\_HGS\_Encryption\_SelfSigned\_Certificate.ps1.



The nCipher Key Storage Provider - Create key wizard appears.



3. In the Create new key panel, select Next.

The **Select a method to protect new key** panel appears.

-	nCipher Key Storage Provider - Create key
	Select a method to protect new key.
	O Module protection (requires no extra cards but is less secure)
	C Softcard protection (unavailable in HSM Pool mode)
	Operator Card Set protection (unavailable in HSM Pool mode)

4. Select the **Operator Card Set protection** and select **Next**.

The **Select token to protect key with** panel appears.

helpher key storage rioti			
Select token to protect	the key with.		
Current Operator Card Sets:	Operator Card Set To	ken Information:	
MSAuthenticode	Name:	MSAuthenticode	
	Token hash:	0x9f595be7	
	Sharing parameters:	1 of 1, Persistent	
	Timeout:	None	
	Currently protecting:	none	
		Net	

5. Present the OCS created before and select Next.

The Choose modules you wish to load the keys onto panel appears.

		×
nCipher Key Storage P	rovider - Create key	
Choose modules yo	u wish to load the key onto.	
Excluded modules:	Included modules:	
Module #2	Add Module #1	
	Remove	
	Add all	
	Remove all	
1		
	<u> </u>	Cancel

- 6. Select the required HSM and select **Add** to move the HSM to the Included modules list. In this example, two HSMs are available.
- 7. Select Finish.

A passphrase dialog appears.

		$\times$
~	nCipher Key Storage Provider	
	Module 1 slot 2: 'MSAuthenticode'	
	#1('MSAuthenticode')	
	You must enter a passphrase for this card	
		_
	******	
	Next Ca	ncel

8. Enter the passphrase for the OCS and select Next.

An OCS status dialog appears.

Card rea	ding com	plete.		
Module	Slot	Content	Status	
1	3 2	Content	complete	
1	0		complete	

9. Select **Finish** after the card reading is completed.

The final command line output will look like the following:

> .\Generate\_HGS\_Encryption\_SelfSigned\_Certificate.ps1

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

 Thumbprint
 Subject

 ----- ----- 

 751A528A88C788458A7A8347543DA58CCC1212A6
 CN=HGS Encryption Certificate

#### 2.4.1.2. Generate signing certificate

To generate a signing certificate:

- 1. Launch PowerShell as Administrator.
- 2. Run the following script: Generate\_HGS\_Singning\_SelfSigned\_Certificate.ps1.

```
$cngProviderName = "nCipher Security World Key Storage Provider"
$subjectName = "HGS Signing Certificate"
$friendlyName = "HGS_Signing_SelfCert"
# $locationName = "Cert:\CurrentUser\My"
$locationName = "Cert:\LocalMachine\My"
New-SelfSignedCertificate -Subject $subjectName -FriendlyName $friendlyName -CertStoreLocation
$locationName -Provider $cngProviderName -KeyUsageProperty Sign -KeyExportPolicy NonExportable
```

3. Select the protection method, present the OCS, select the HSM, and enter the passphrase when prompted. This is similar process to the previous section.

The final command line output will look like the following:



#### 2.4.2. Confirm certificates and keys

When keys are generated by the HSM:

- The key's blobs are stored in the C:\ProgramData\nCipher\Key Management Data\local directory.
- On the HGS the certificates are in the \LocalMachine\My store directory.

To verify that the certificates are in the correct location using PowerShell:

> Get-ChildItem Cert:\LocalMachine\My -DnsName hgs\*

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint Subject
E59DFA33163C4DB47E74039249BCCBF3B857C17F CN=HGS Signing Certificate
751A528A88C788458A7A8347543DA58CCC1212A6 CN=HGS Encryption Certificate

To verify the certificates via the command line, use **certutil** (see below). Present the OCS, select the HSM, and enter the passphrase when prompted. For example:



Make a note of the **Cert Hash(sha1)** values for the signing certificate and the encryption certificate. You will use these in the next section.

## 2.5. Initialize the Host Guardian Service

To initialize the Host Guardian Service:

- 1. Launch PowerShell as Administrator.
- 2. Run the following script: Initialize\_HGS\_Server\_Trust\_Host\_Key.ps1.

\$hgsServiceName = "HGS"

\$encryptionCertificateThumbprint = "751A528A88C788458A7A8347543DA58CCC1212A6"

\$signingCertificateThumbprint = "E59DFA33163C4DB47E74039249BCCBF3B857C17F"

Initialize-HgsServer -HgsServiceName \$hgsServiceName -EncryptionCertificateThumbprint
\$encryptionCertificateThumbprint -SigningCertificateThumbprint \$signingCertificateThumbprint -TrustHostKey

In this script:

- For hgsServiceName, insert a name of your choosing for the HGS node. This name will be the distributed network name of the cluster and should not be fully qualified. For example, enter HGS if you want the FQDN to be configured as HGS.<domain>.<com>.
- For encryptionCertificateThumbprint, insert the encryption certificate hash from Confirm certificates and keys.
- For signingCertificateThumbprint, insert the signing certificate hash from Confirm certificates and keys.

<pre>&gt; .\Initialize_HGS_Server_Trust_Host_Key.ps1 WARNING: The names of some imported commands from the module 'BitLocker' include unapproved verbs that might make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb. LogPath: C:\Windows\Logs\HgsServer\220714101502\HOSTGUARDIANSRV WARNING: Ensure that service account 'hgs\HGSSVC_64C43\$' has read access to the private key of certificate with thumbprint '751A528A88C788458A7A8347543DA58CCC1212A6', and that that the private key is both present and accessible on all Host Guardian Service servers. WARNING: Ensure that service account 'hgs\HGSSVC_64C43\$' has read access to the private key of certificate with thumbprint 'E59DFA33163C4DB47E74039249BCCBF38857C17F', and that that the private key is both present with thumbprint 'E59DFA33163C4DB47E74039249BCCBF38857C17F', and that that the private key is both present with thumbprint 'E59DFA33163C4DB47E74039249BCCBF38857C17F', and that that the private key is both present with thumbprint 'E59DFA33163C4DB47E74039249BCCBF38857C17F', and that the private key is both present with thumbprint 'E59DFA33163C4DB47E74039249BCCBF38857C17F', and that the private key is both present with thumbprint 'E59DFA33163C4DB47E74039249BCCBF38857C17F', and that the private key is both present with thumbprint 'E59DFA33163C4DB47E74039249BCCBF38857C17F', and that the private key is both present with thumbprint 'E59DFA33163C4DB47E74039249BCCBF38857C17F', and that that the private key is both present with thumbprint 'E59DFA33163C4DB47E74039249BCCBF38857C17F', and that that the private key is both present with thumbprive that the private key is both present with thumbprive that the private key is both present with thumbprive that the private key is both present with thumbprive the the private key is both present with thumbprive the the private key is both present with thumbprive the the private key is both present with thumbprive the</pre>
with thumbprint 'E59DFA33163C4DB47E74039249BCCBF3B857C17F', and that that the private key is both present and accessible on all Host Guardian Service servers.

- 3. Make a note of the name of the service account that is created during this process.
- 4. Ensure the service account created above has rights to the HSM backed keys:
  - a. Launch the IIS Manager and select **Application Pools** and note the Identity under which the **KeyProtection app pool** is running. For example:

💐 Internet Information Services (IIS) Manager						
← → @ ► HOSTGUARDIANSRV ► App	lication Pools					
File View Help						
Connections Q • ↓ 2 00. Q Tast Page V Q HOSTGUARDIANSRV (hg:\Administrator) ↓ Q Application Pools > ↓ Sites	Applicat This page lets you vie are associated with wi among different appli	w and man orker proce cations.	DIS age the list of ap sses, contain on Go - 🗔 Sho	plication pools on e or more applicati w All Group by:	the server. Application po ons, and provide isolation No Grouping	ool n
	Name	Status	.NET CLR V	Managed Pipel	Identity	1
	.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdent	C
	.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdent	C
	AttestationApp	Started	v4.0	Integrated	ApplicationPoolIdent	1
	DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdent	1
	C KeyProtection	Started	v4.0	Integrated	hgs\HGSSVC_64C43\$	1

b. Run the Local Machine Certificate Management Console certlm.msc.
 Locate the encryption certificate under the Personal folder.

- c. Right-click and select **All tasks > manage Private keys**.
- d. Present the OCS, select the HSM, and enter the passphrase when prompted.
- e. Add the service account above to the list of Groups and Users permitted to manage the private keys.
- f. Select Add > Object Types > Service Accounts, then select OK.
- g. Under **Enter the object names to select**, type the account name. The default is **HGSSVC**.
- h. Select Check Names.



 Give the service account Read access to the private keys for the certificate. To do this, select **Advanced**, select the user account, then select **Edit**. For example:

ermission Auditing armission entry. To modify a permission entry, select the entry and click Edit (if available), ermission entries: Type Principal Access Inherited from Allow HGSSVC, 64C435 (hgs\HGSSVC, 64C435) Read None Allow STSTM Full control Parent Object Allow Jsers (hgs\Users) Read Parent Object Allow Users (hgs\Users) Read Parent Object Allow Remove Edit	wner:		Administrators (hgs\Administrators) Cha	nge				
ar additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available), strainistion entries: Type Principal Access Inherited from Allow HGSSVC_64C435 (hgs\HGSSVC_64C435) Read None Allow STSTM Full control Parent Object Allow Jusers (hgs\Users) Read Parent Object Allow Users (hgs\Users) Read Parent Object	ermis	sions	Auditing					
Intervision entries: Type Principal Access Inherited from Allow HGSSVC_64C435 (hgs\HGSSVC_64C435) Read None Allow STSTM Full control Parent Object Allow Administrators (hgs\Administrators) Full control Parent Object Allow Users (hgs\Users) Read Parent Object Add Remove Edit	or add	ditiona	al information, double-click a permission entr	y. To modify a permission	n entry, select the entry and clic	c Edit (if ava	ilable).	
Type     Principal     Access     Inherited from       Allow     HGSSVC_64C435 (hgs\HGSSVC_64C435)     Red     None       Allow     STEM     Full control     Parent Object       Allow     VSTM     Full control     Parent Object       Allow     Users (hgs\Users)     Read     Parent Object	ermis	sion e	ntries:					
Allow     HOSSVC_64C435 (hgs/HGSSVC_64C435)     Read     None       Allow     SYSTEM     Full control     Parent Object       Allow     Allow     Home     Parent Object       Allow     Users (hgs/Users)     Read     Parent Object	Ty	pe	Principal	Access	Inherited from			_
Allow     SYSTEM     Full control     Parent Object       Allow     Administrators (hgs/Vdministrators)     Full control     Parent Object       Allow     Users (hgs/Users)     Read     Parent Object	All	low	HGSSVC_64C43\$ (hqs\HGSSVC_64C43\$)	Read	None			
Allow Administrators (hgs/Administrators) Full control Parent Object Allow Users (hgs/Users) Read Parent Object	All	low	SYSTEM	Full control	Parent Object			
Allow Users (hgs\Users) Read Parent Object	AII	low	Administrators (hgs\Administrators)	Full control	Parent Object			
Add Remove Edit	All	low	Users (hgs\Users)	Read	Parent Object			
Add Remove Edit								
Add Remove Edit								
Add Remove Edit								
Add Remove Edit								
Add Remove Edit								
Add Remove Edit								_
	Ac	dd	Remove Edit					

j. Repeat the process for the signing certificate.

# 2.6. Configure the Guarded Host

The Guarded Host is the host server for the Hyper-V virtual machines that will become Shielded VMs. The Guarded Host will require attestation from the HGS

before its shielded VMs will be allowed to run. For the purpose of this guide, the Guarded Host was implemented on a ESXi 7.1 VM.

- 1. On the ESXi Hypervisor, edit VM settings.
- On the Virtual Hardware tab, ensure that Expose hardware assisted virtualization to guess OS is selected. For example:

	ADD NEW	DEVICE
CPU	2 ~	(j)
Cores per Socket	2 × Sockets: 1	
CPU Hot Plug		
Reservation	0 ~ MHz ~	
Limit	Unlimited V MHz V	
Shares	Normal ~ 2000	
Hardware virtualization	$\ensuremath{\boxtimes}$ Expose hardware assisted virtualization to the guest OS	i
Performance Counters	Enable virtualized CPU performance counters	
I/O MMU	Enabled	

3. On the VM Options tab, ensure that Virtualization Based Security is enabled.

Hardware VM Options	
General Options	VM Name: Microsoft_Host_Guardian_Host
VMware Remote Console Options	Lock the guest operating system when the last remote user disconnects
Encryption	Expand for encryption settings
Power management	Expand for power management settings
VMware Tools	Expand for VMware Tools settings
Virtualization Based Security	⊡ Enable
Boot Options	Expand for boot options
Advanced	Expand for advanced settings
Fibre Channel NPIV	Expand for Fibre Channel NPIV settings

- 4. Ensure that the following roles are installed:
  - AD DS
  - DNS
  - AD LDS.

This is required for **netdom.exe** which is used to establish one-way trust from the HGS to the Fabric domain.

• Hyper-V.

This should include the Host Guardian support feature.

 Determine the status of the required roles by selecting Add Roles and Features Server Selection > Server Roles. The installed features are selected. For example:

Add Roles and Features Wizard		- X DESTINATION SERVER HostGuardianHist
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select one or more roles to install on the selected server.	Description Active Directory Certificate Services (AD C5) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	< Previous Next >	Install

- 6. Ensure the hypervisor-protected code integrity (HVCI) is enabled, see Enable virtualization-based protection of code integrity.
- 7. Promote the DNS server as normal if installing it for the first time.

Deployment Configuration         Domain Controller Options         Additional Options         Paths         Review Options         Prerequisites Check         Instaliation         Results         Select the deployment operation         Add a domain controller to an existing domain         Add a new domain to an existing forest         Add a new forest         Specify the domain information for this operation         Precequisities Check         Installation         Results         Supply the credentials to perform this operation	TARGET SERVEF HostGuardianHs
Deployment Configuration           Domain Controller Options           Additional Options           Add a new domain to an existing domain           Add a new domain to an existing forest           Add a new forest           Review Options           Prerequisites Check           Installation           Results           Forest name:           New domain name:           Guardedhost.com           Supply the credentials to perform this operation	
hgs/Administrator	v Change
More about deployment configurations	

- 8. Add the Host Guardian Server DNS as a conditional forwarder:
  - a. Open PowerShell as Administrator
  - b. Run the following script named

Add\_DNS\_Server\_Conditional\_Forward\_Zone.ps1.

<pre>\$hgsDomainName = "hgs.com"</pre>	
<pre>\$ipAddressHGSServer = "xxx.xxx.xxx"</pre>	
Add-DnsServerConditionalForwarderZone -Name <pre>\$hgsDomainName -ReplicationScope "Forest" -MasterServers</pre> \$ipAddressHGSServer	



This can also be performed from the DNS Manager GUI.

- 9. Set the Guarded Host domain to trust the Guardian Server domain:
  - a. Open a CLI as Administrator.
  - b. Run the following command:



- 10. Generate a Guardian Host key automatically or select an existing certificate. Alternatively, you can also use a certificate generated by the nShield HSM as on the Guardian Server.
  - a. Open PowerShell as Administrator.
  - b. Run the following command:

> Set-HgsClientHostKey

c. Get the public half of the key to provide the HGS server.

You can also provide a .cer file that contains the public half of the key. Note that the HGS is only used to store and validate the public key. No certificate information is stored on the HGS and neither the certificate chain nor the expiration date is validated by the HGS.

Open PowerShell as Administrator and run:



- d. Copy the listed certificate file to the Guardian Server using the method of your choice. You will add this certificate to the attestation service.
- 11. Create a new Global security group to identify the Guarded Hosts that will run the shielded VMs.
  - a. Open the Server Manager and select **Tools >Active Directory Users and Computers**.
  - b. Expand the domain.

c. Right-click **Users**, select **New > Group**, and enter the group name.

New Object - Group			$\times$
Create in: guardedhost.	.com/Users		
Group name:			
Guarded Hosts			
Group name (pre-Windows 2000):			
Guarded Hosts			
Group scope	Group typ	e	
○ Domain local	<ul> <li>Securit</li> </ul>	y	
Isologia	⊖ Distribu	ition	
○ Universal			
		OK	Cancel

The security group is created. For example:

Active Directory Users a File Action View Hele	and Computers p   🗙 🖾 @ 🐟 📓 📷 🔏 🎕	l in 🍸 🧕 🕷	-	<
Active Directory Users a Saved Queries Saved Queries Builtin Builtin Builtin Computers Builtin Computers Builtin Computers Builtin Computers Managed Servic Users Servic	Name Construction Construction Construction Construction Construction Construction Construction Controllers Comain Controllers Comain Guests Comain Guests Comain Guests Comain Users Construction Controllers Construction Constr	Type Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description Members in this group c DNS Administrators Group DNS clients who are per Designated administrato All workstations and serv All domain controllers in All domain guests All domain users Members in this group c	^
	Guest	User Security Group	Built-in account for gues Members of this group c	
< >>	<	Security Group	weinsels of this group ta	Í

- 12. Get the Security Identifier (SID) of the security group created above.
  - a. Open PowerShell as Administrator.
  - b. Run the following command:

> Get-ADGroup "Gua	rded Hosts"
DistinguishedName GroupCategory	: CN=Guarded Hosts,CN=Users,DC=guardedhost,DC=com : Security
GroupScope	: Global
Name	: Guarded Hosts
ObjectClass	: group
ObjectGUID	: b914cb31-fe5f-4d10-be70-60bbcfa95243
SamAccountName	: Guarded Hosts
SID	: S-1-5-21-2491135030-878028546-2245137482-1104

## 2.7. Configure attestation on the Guardian Server

Perform the following on the Guardian Server:

- 1. Register the global security group created in the Guarded Host with the Guardian Server as an Attestation Host Group:
  - a. Copy the group name and SID from the previous step.
  - b. Open PowerShell as Administrator and run the Register\_Security\_Group\_with\_Guardian\_Server.ps1 script.

```
$guardedHostName = "Guarded Hosts"
$SID = "S-1-5-21-2491135030-878028546-2245137482-1104"
Add-HgsAttestationHostGroup -Name $guardedHostName -Identifier $SID
```

The command line and output look like the following:

```
> .\Register_Security_Group_with_Guardian_Server.ps1
WARNING: The current attestation operation mode is: "HostKey". Any "AD" mode specific changes made or
content returned will not take effect until the attestation operation mode is changed to "AD".
S-1-5-21-2491135030-878028546-2245137482-1104:Guarded Hosts
```

2. Confirm that the Guarded Host group was added:

```
> Get-HgsAttestationHostGroup
WARNING: The current attestation operation mode is: "HostKey". Any "AD" mode specific changes made or
content returned will not take effect until the attestation operation mode is changed to "AD".
Name Identifier
---- Identifier
Guarded Hosts S-1-5-21-2491135030-878028546-2245137482-1104
```

Notice the returned friendly name and SID.

This completes the process of configuring the HGS cluster.

- 3. Add the Guardian Host certificate copied above to the attestation service. The certificate was copied to C:\Users\Administrator\Documents.
  - a. Open PowerShell as Administrator.
  - b. Run the following command:



4. The fabric Administrator needs to provide two URLs from the Guardian Server to the Guarded Host. Obtain these URLs by executing the following command:

> Get-HgsServer	
Name	Value
AttestationOperationMode	HostKey
AttestationUrl	{http://hgs.hgs.com/Attestation}
KeyProtectionUrl	{http://hgs.hgs.com/KeyProtection}

## 2.8. Configure attestation on the Guarded Host

Perform the following on the Guarded Host:

- 1. Configure the Key Protection and Attestation URLs.
- 2. Open PowerShell as Administrator and run the following cmdlet.

Set-HgsClientConfiguration - http://hgs.hgs.com/KeyProtect	AttestationServerUrl 'http://hgs.hgs.com/Attestation'-KeyProtectionServerUrl ion'
IsHostGuarded	: True
Mode	: HostGuardianService
KeyProtectionServerUrl	: http://hgs.hgs.com/KeyProtection
AttestationServerUrl	: http://hgs.hgs.com/Attestation
AttestationOperationMode	: HostKey
AttestationStatus	: Passed
AttestationSubstatus	: NoInformation
FallbackKeyProtectionServerUrl	:
FallbackAttestationServerUrl	:
IsFallbackInUse	: False

3. Copy the attestation server URL and key protection server URL from the previous step.

You should now be able to create shielded VM templates as per Microsoft guidelines using either Virtual Machine Manager (VMM) or Windows Azure Pack.

# Chapter 3. Troubleshooting

The following table lists error messages that might appear during the procedures described in this guide.

Problem	Cause	Solution
nfkminfo.exe reports !Usable State = unchecked	Module does not have a valid Security World loaded.	Reload the Security World onto the HSM Refer to the HSM <i>User Guide</i> for full details. Ensure that you have the Administrator Card quorum and passwords. Place the HSM into Initialisation mode and run the new-world command

Problem	Cause	Solution
nfkminfo.exe reports !Usable State = foreign	Module does not have the correct world file. The world file is from an unrecognized Security World. The world file in the C:\ProgramData\nCipher\Key Management Data\local directory is incongruous to the Security World loaded onto the HSM.	Ensure that you are using the correct world file. If you are using multiple Security Worlds in your environment, you must ensure that you use the appropriate Security World file that corresponds to the Security World loaded on the HSM. For help with using multiple Security Worlds, contact Entrust nShield Support, https://nshieldsupport.ent rust.com. [NOTE] Access to the Entrust Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.c om.
<b>nShield Edge only</b> When using an nShield USB attached Edge HSM, the Edge is not reported as available or is reported as failed.	This is due to an outdated USB driver used by the nShield Edge.	Open a command window as an Administrator and navigate to %nfast_home%\bin. Run nc_hsc.exe to restart the hardserver service. The driver can be updated from the FTDI website.

<b>nShield Edge only</b> nShield Security World This has no impact on the Version 12.xx and newer HSM nor Security World	Problem	Cause	Solution
When you run enquiry, nShield Edge reports hardware Status as unsupported Driverexpects to be able to read the HSM Hardware status (error codes). The Edge does not support this function and therefore responds with the unsupported driver hardware status.and can safely be ignore no remedial action is required.	nShield Edge only When you run enquiry, nShield Edge reports hardware Status as unsupported Driver	nShield Security World Version 12.xx and newer expects to be able to read the HSM Hardware status (error codes). The Edge does not support this function and therefore responds with the <b>unsupported driver</b> hardware status.	This has no impact on the HSM nor Security World and can safely be ignored. No remedial action is required.

# Chapter 4. Remote Administration

Remote Administration uses smartcards and a Trusted Verification Device. Before any smartcard can be used, it must be registered in the acceptable card white list.

For added security, each smartcard's unique serial number can be entered. The serial number is the 16-digit number found at the bottom of the card. You can allow any smartcard with the wildcard character (\*).

Save the cardlist and close the cardlist configuration file.

Initially these smartcards will form your Administrator Card Set. For information about ACS, see the *User Guide* for your HSM.

The cardlist configuration file can be found in: C:\ProgramData\nCipher\Key Management Data\config\cardlist.



By default, ProgramData is hidden. In Windows Explorer, select View, then select Hidden items.

Example cardlist configuration file: