Member of
Microsoft Intelligent
Security Association

Microsoft Security

Microsoft Host Guardian Service and Shielded Virtual Machines

nShield® HSM Integration Guide

2023-12-05

Table of Contents

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	✓	✓	✓
Connect XC	12.80.4	12.50.11 (FIPS Certified)	12.80.4	✓	✓	✓
Connect XC	12.80.4	12.72.1 (FIPS Certified)	12.80.5	✓	✓	✓
nShield 5c	13.2.2	13.2.2 (FIPS Pending)	13.2.2	✓	✓	✓

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

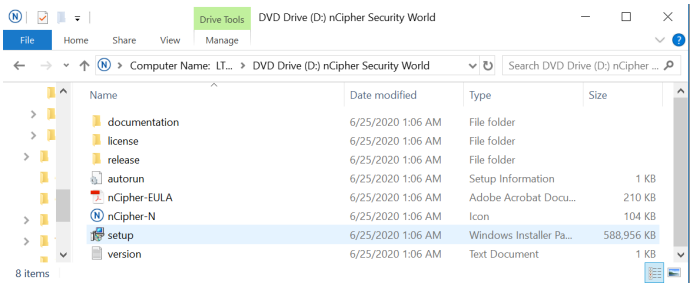
1. Install the Security World software on the Guardian Server:

    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.



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

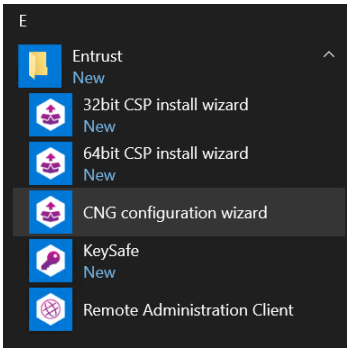
It is necessary to install and register the nShield Cryptography API: Next Generation (CNG) provider on the Guardian Server. This can be done using either the command line or the **CNG Configuration** wizard.

Before proceeding, check that no legacy providers are installed.

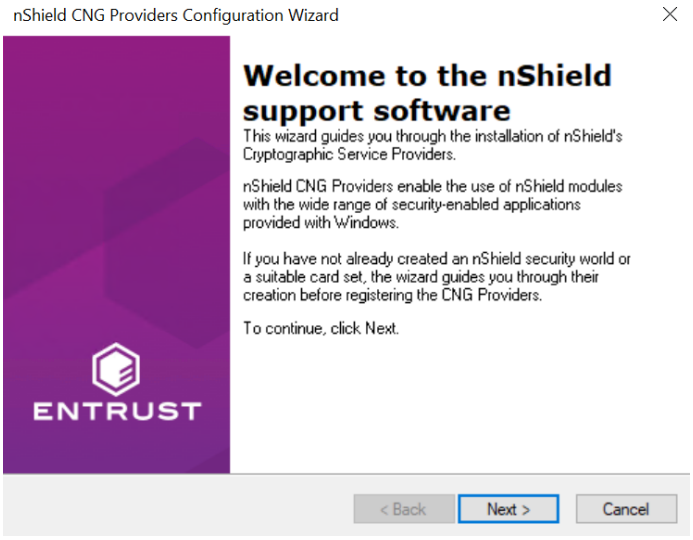
1. Run the command:

```
>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 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
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.

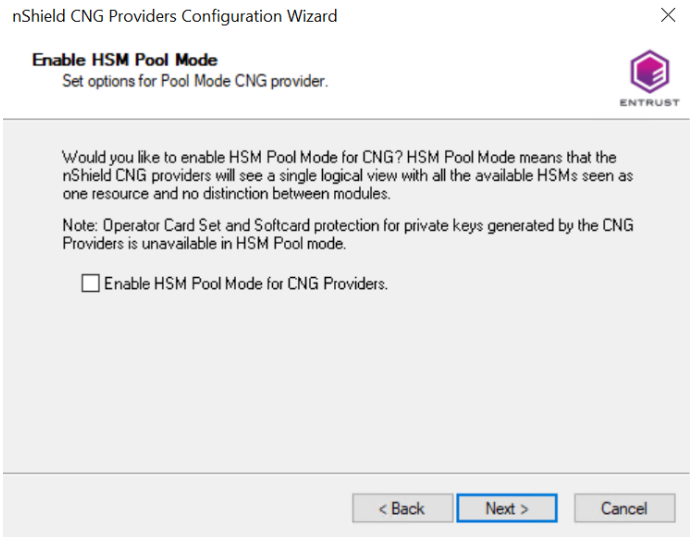


The **nShield CNG Providers Configuration Wizard** starts.



4. On the **Welcome** panel, select **Next**.

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



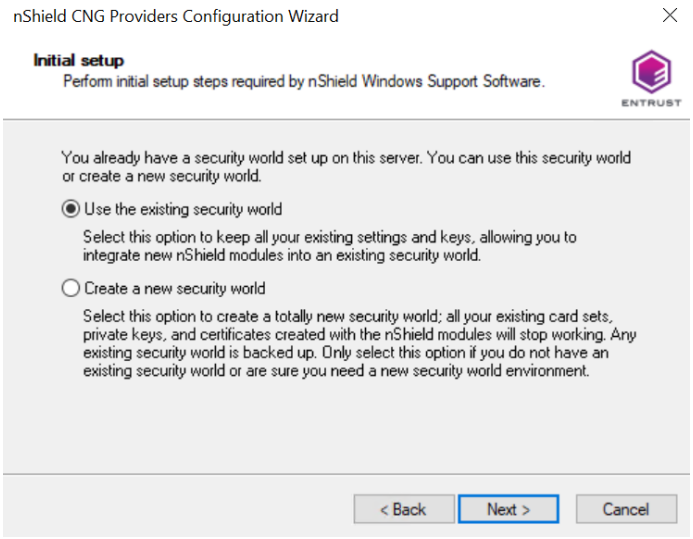
5. If you intend to use multiple HSMs in a failover and load-sharing capacity, select **Enable HSM Pool Mode for CNG Providers**. If you do, you can only use

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:

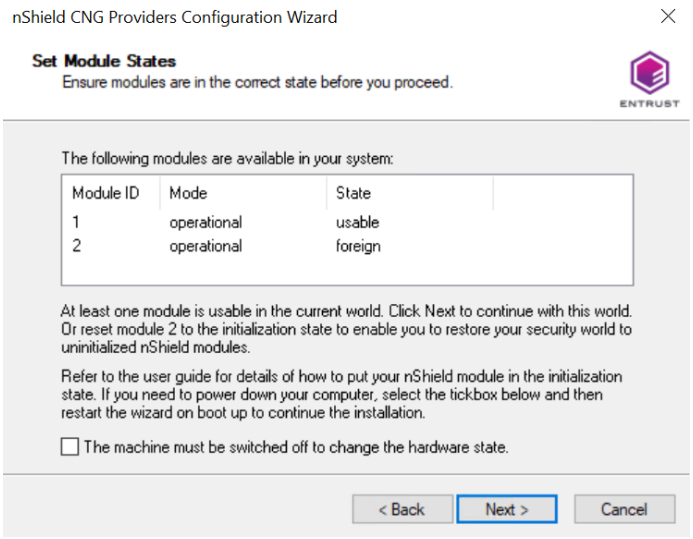


   - Select **Use the existing security world** if you already have a Security World that you intend to use. The corresponding `world` and `module_xxxx-xxxx-xxxx` files must be present in the `%NFAST_KMDATA%\local` directory. Be prepared to present the quorum of Administrator cards.
   - Select **Create 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.

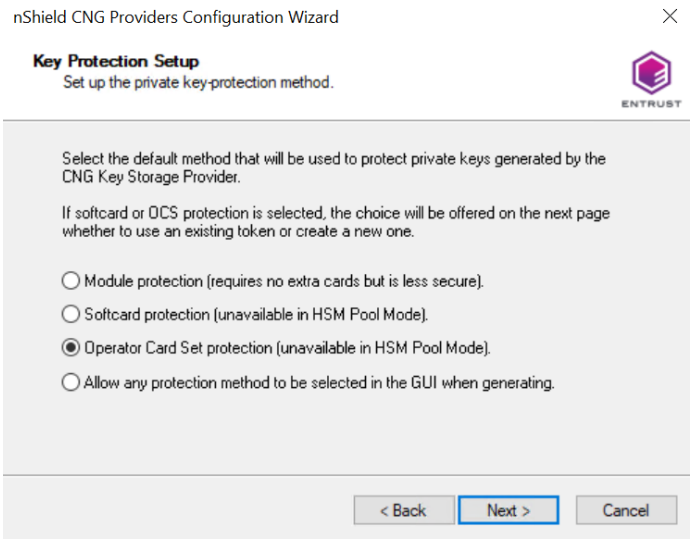
7. Select **Next**.

   The **Set Module States** panel appears.



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

   The **Key Protection Setup** panel appears.

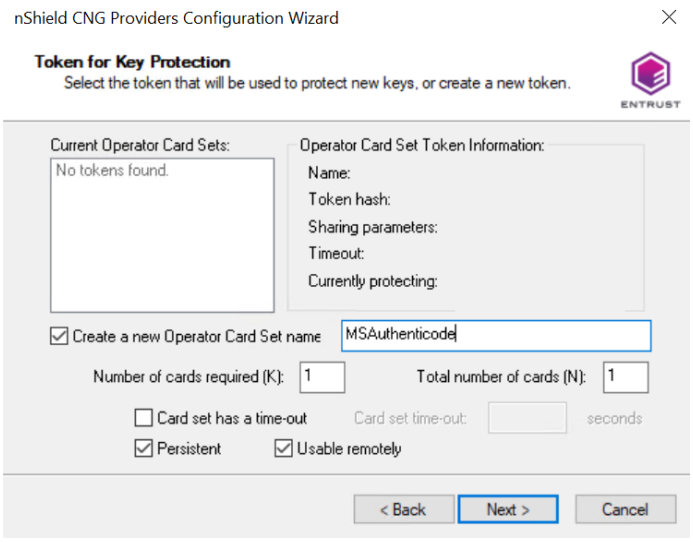


10. Select the required protection method.

    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.

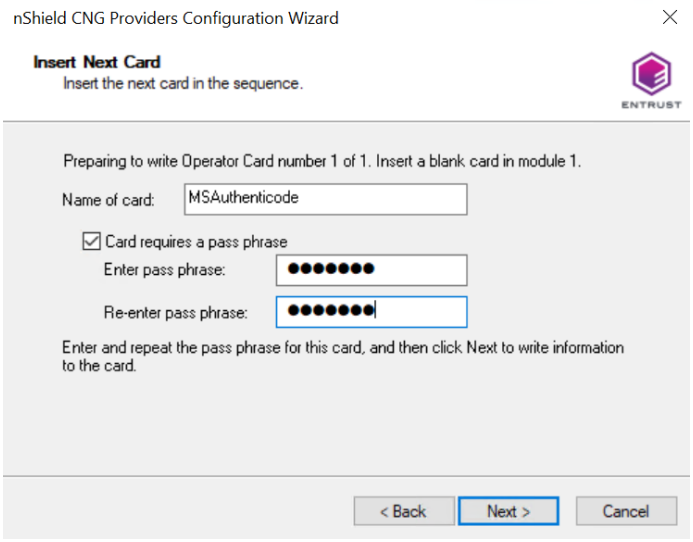


12. Enter the OCS name, K and N values, select **Persistent**, and select **Usable remotely**.
13. Select **Next**.

    You must now present the cards.

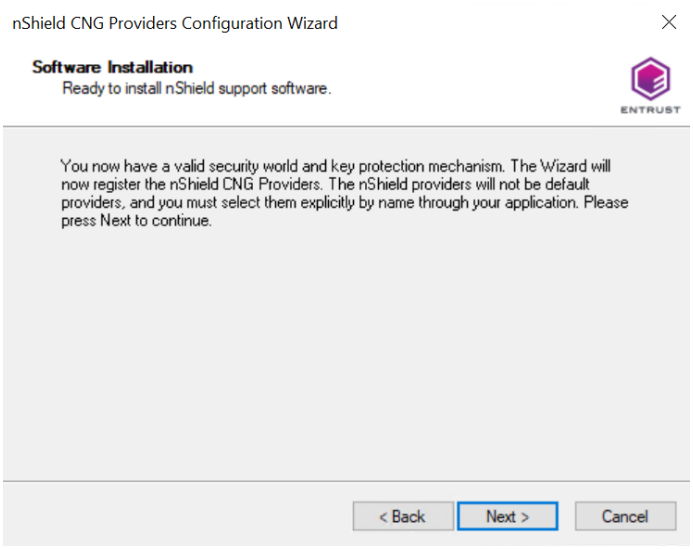
14. First present the ACS to the HSM.

    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.



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.



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

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.

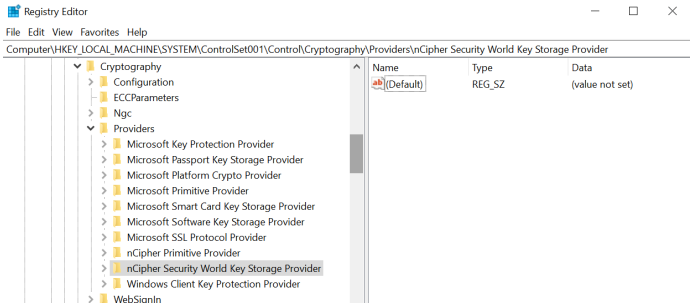
18. Run the following from PowerShell after the Host Guardian Service has been installed:

```
> 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
```

19. 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/en-us/windows-server-docs/security/guarded-fabric-shielded-vm/guarded-fabric-deploying-hgs-overview.

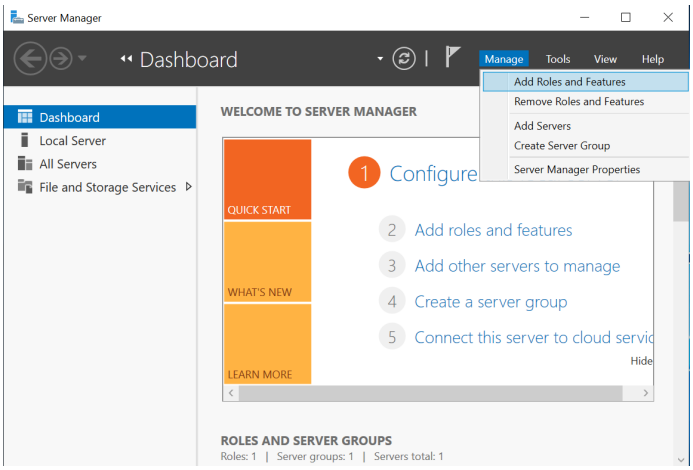
2.3.1. Add the Host Guardian Server role using the Server Manager GUI

You can also add the Host Guardian Server role using

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

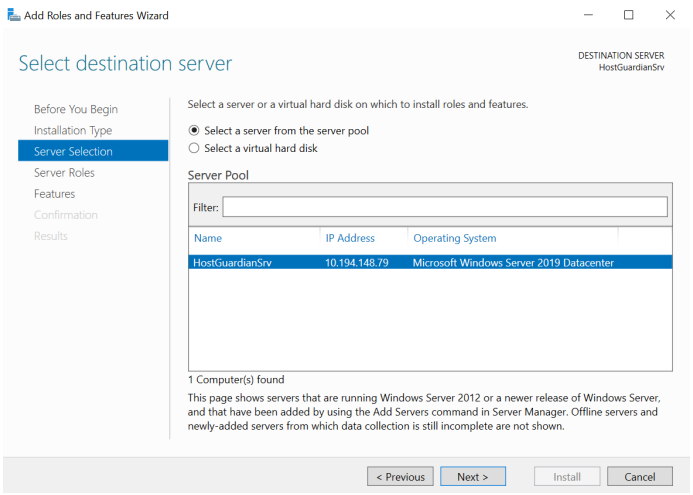
To add the Host Guardian Server using the Server Manager GUI:

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:

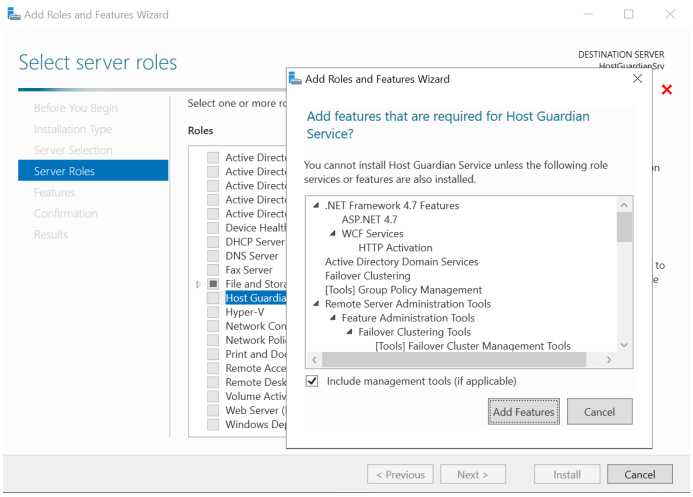


4. Select **Next**.

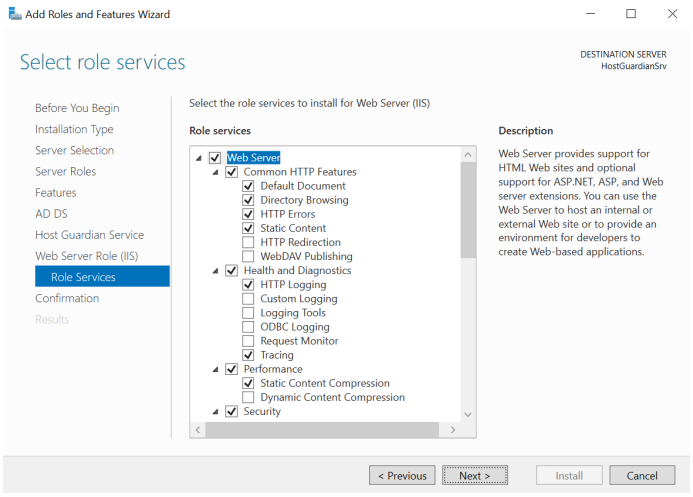
   The **Select server roles** panel appears.

5. Select **Host Guardian Service**.

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



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.

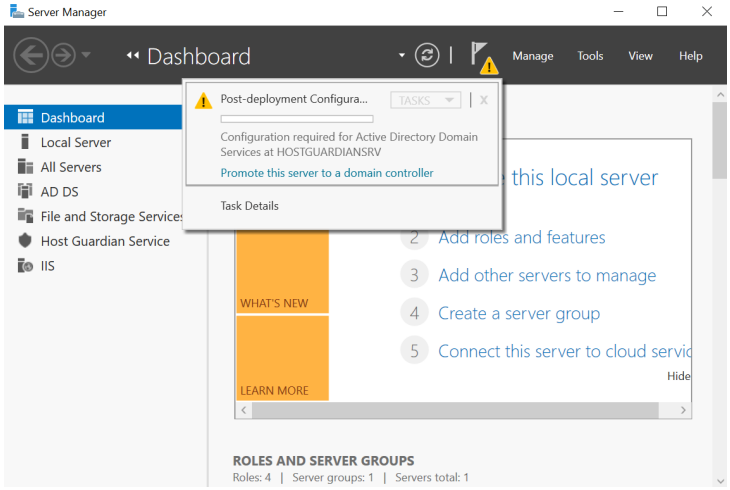


8. Select **Next** to install IIS and then select **Install**.

   After the installation completes, a server restart is required.

After the role has been added, you are prompted to continue with **Post-deployment 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.



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.

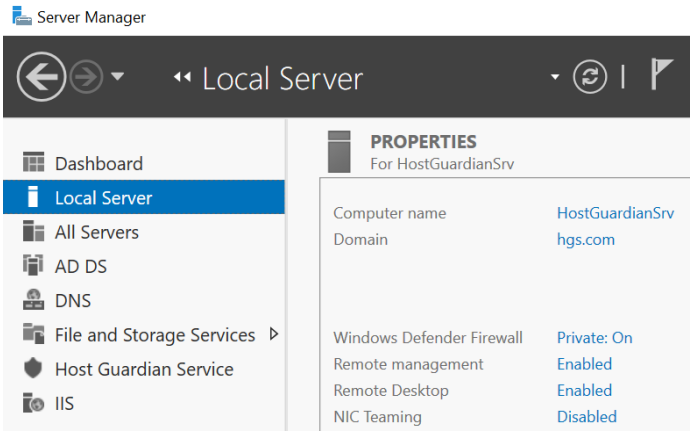
```
$hgsDomainName = "hgs.com"

$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.

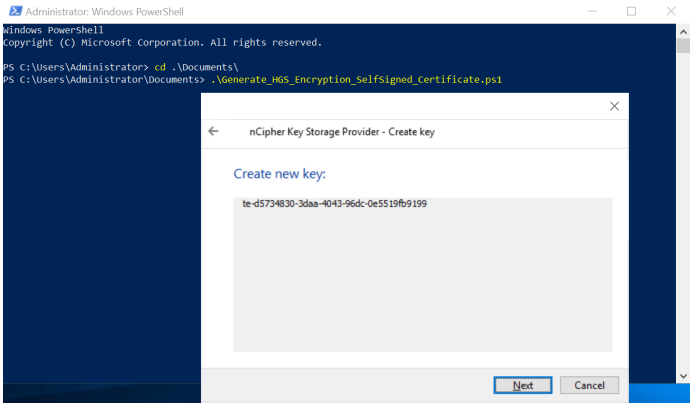
2.4.1.1. Generate encryption certificate

To generate an encryption certificate:

1. Launch PowerShell as Administrator.
2. Run the following script: `Generate_HGS_Encryption_SelfSigned_Certificate.ps1`.

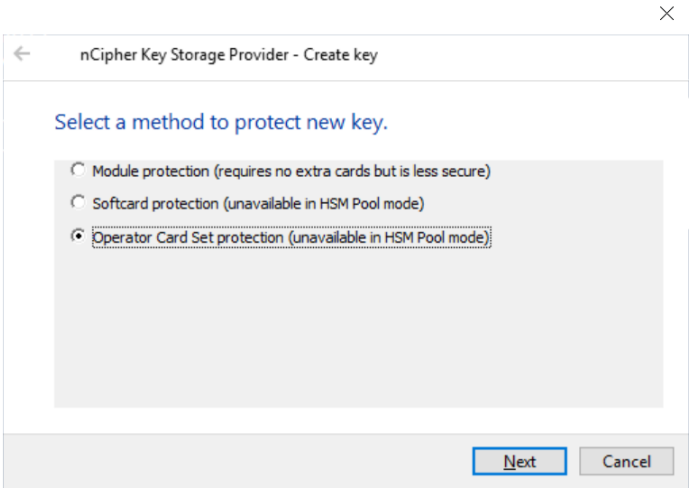
```
$cngProviderName = "nCipher Security World Key Storage Provider"

$subjectName = "HGS Encryption Certificate"

$friendlyName = "HGS_Encryption_SelfCert"

# $locationName = "Cert:\CurrentUser\My"
$locationName = "Cert:\LocalMachine\My"

New-SelfSignedCertificate -Subject $subjectName -FriendlyName $friendlyName -CertStoreLocation
$locationName -Provider $cngProviderName -KeyExportPolicy NonExportable
```

   The **nCipher Key Storage Provider - Create key** wizard appears.



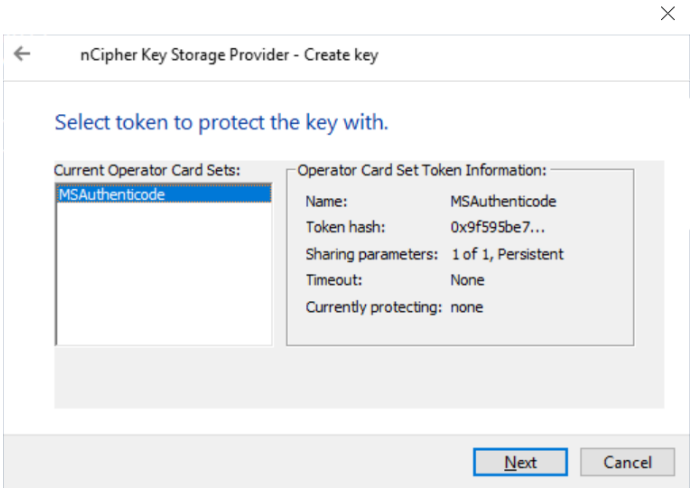
3. In the **Create new key** panel, select **Next**.

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



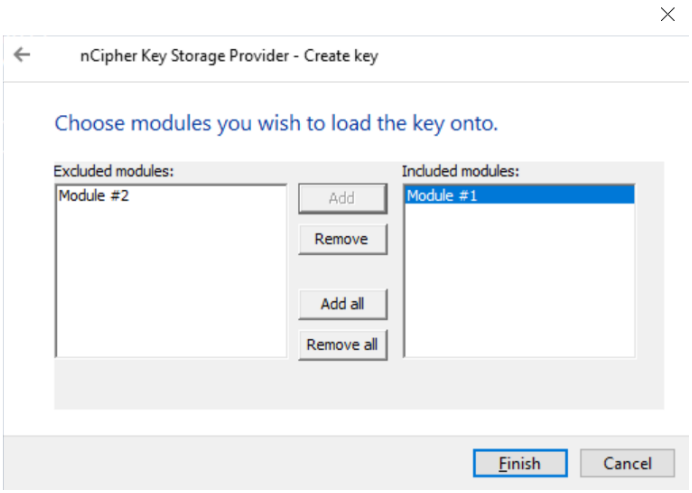
4. Select the **Operator Card Set protection** and select **Next**.

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



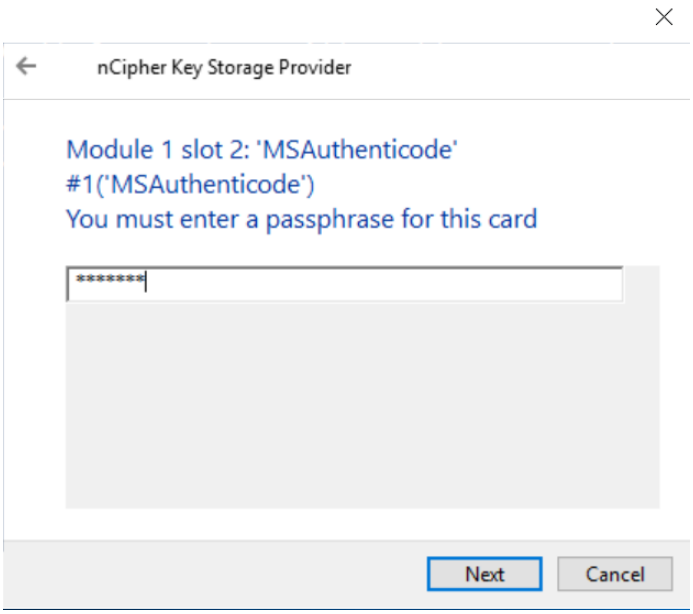
5. Present the OCS created before and select **Next**.

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



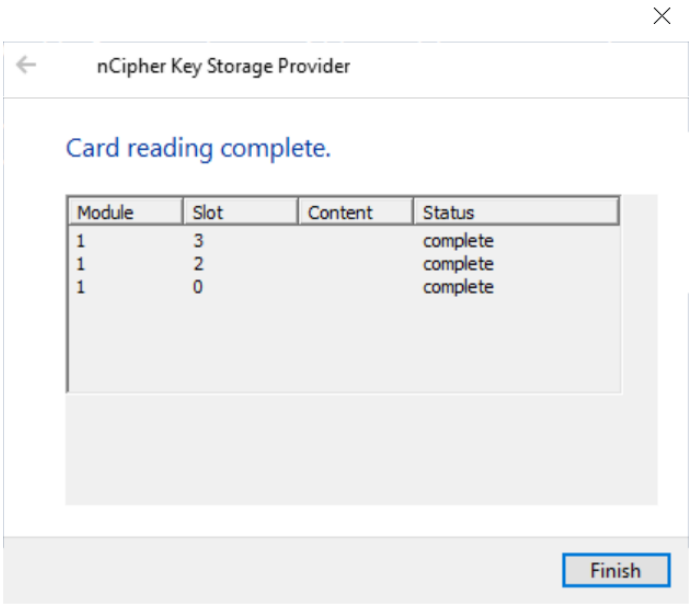
6. Select the required HSM and select **Add** to move the HSM to the Included modules list. In this example, two HSMs are available.
7. Select **Finish**.

   A passphrase dialog appears.



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

   An OCS status dialog appears.



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:

```
> .\Generate_HGS_Singning_SelfSigned_Certificate.ps1


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

Thumbprint                                Subject
----------                                -------
E59DFA33163C4DB47E74039249BCCBF3B857C17F  CN=HGS Signing Certificate
```

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:

```
C:\Users\Administrator>certutil -store my
my "Personal"
================ Certificate 0 ================
Serial Number: 31c30a8d8e0246bd47f29d91d5780d7d
Issuer: CN=HGS Signing Certificate
 NotBefore: 7/14/2022 9:07 AM
 NotAfter: 7/14/2023 9:27 AM
Subject: CN=HGS Signing Certificate
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): e59dfa33163c4db47e74039249bccbf3b857c17f
  Key Container = te-418055d2-40a0-47da-8cbf-b1c6ca224cea
  Provider = nCipher Security World Key Storage Provider
Private key is NOT exportable
Signature test passed

================ Certificate 1 ================
Serial Number: 2082cc9faf4fa19742745ae548ad1055
Issuer: CN=HGS Encryption Certificate
 NotBefore: 7/13/2022 5:26 PM
 NotAfter: 7/13/2023 5:46 PM
Subject: CN=HGS Encryption Certificate
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 751a528a88c788458a7a8347543da58ccc1212a6
  Key Container = te-d5734830-3daa-4043-96dc-0e5519fb9199
  Provider = nCipher Security World Key Storage Provider
Private key is NOT exportable
ERROR: Could not verify certificate public key against private key
CertUtil: -store command completed successfully.
```

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"
```

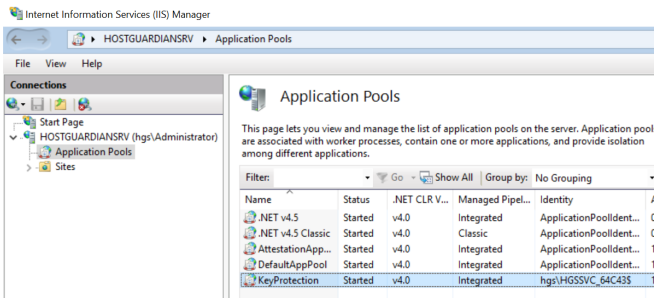
```
$encryptionCertificateThumbprint = "751A528A88C788458A7A8347543DA58CCC1212A6"

$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.

```
> .\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 '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:



   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**.

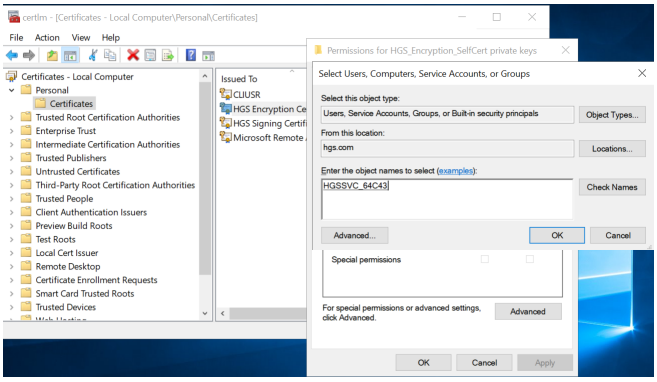
d. Present the OCS, select the HSM, and enter the passphrase when prompted.

e. Add the service account above to the list of Groups and Users permitted to manage the private keys.

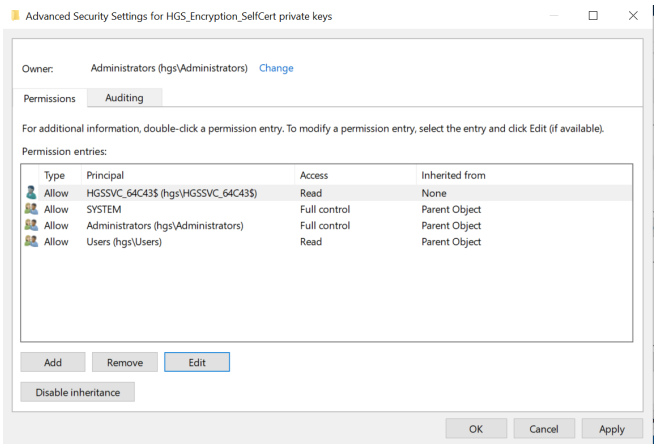
f. Select **Add > Object Types > Service Accounts**, then select **OK**.

g. Under **Enter the object names to select**, type the account name. The default is **HGSSVC**.

h. Select **Check Names**.



i. 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:



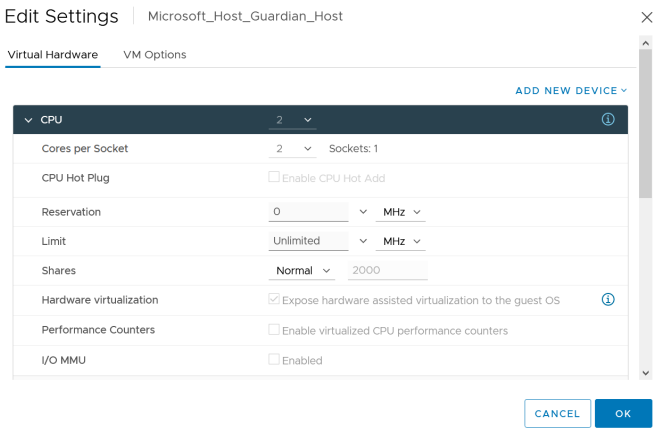
j. Repeat the process for the signing certificate.

2.6. Configure the Guarded Host

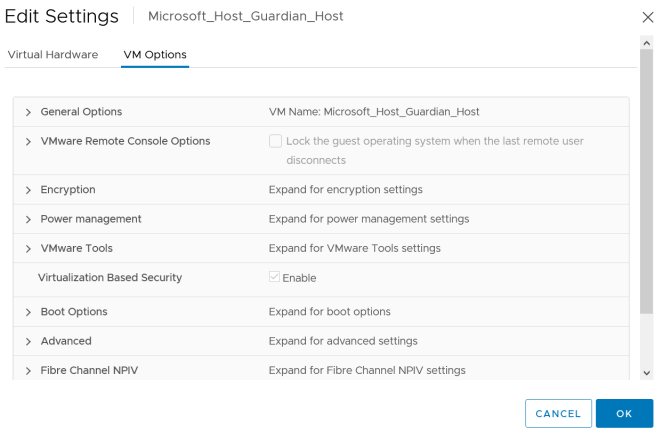
The Guarded Host is the host server for the Hyper-V virtual machines that will become Shielded VMs. The Guarded Host will require attestation from the HGS

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.
2. On the **Virtual Hardware** tab, ensure that **Expose hardware assisted virtualization to guess OS** is selected. For example:



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



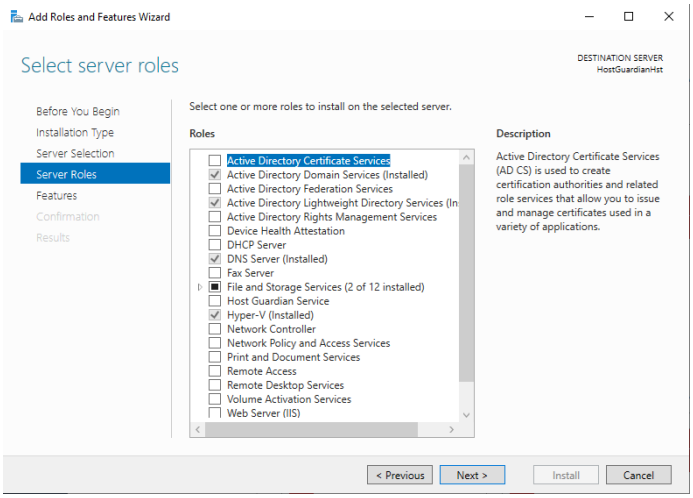
4. Ensure that the following roles are installed:
    - AD DS
    - DNS
    - AD LDS.

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

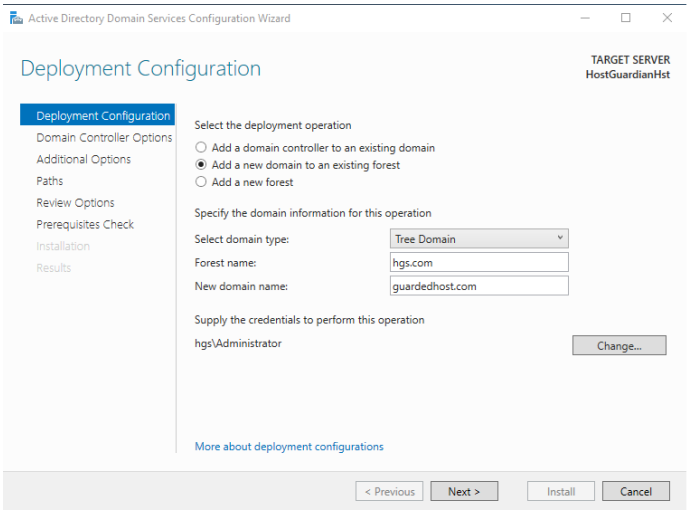
    - Hyper-V.

      This should include the Host Guardian support feature.

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



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.



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`.

```
$hgsDomainName = "hgs.com"

$ipAddressHGSServer = "xxx.xxx.xxx.xxx"

Add-DnsServerConditionalForwarderZone -Name $hgsDomainName -ReplicationScope "Forest" -MasterServers
$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:

```
>netdom trust guardedhost.com /domain:hgs.com /userd:hgs\Administrator /passwordd:nCipher123! /add

The command completed successfully.
```

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.

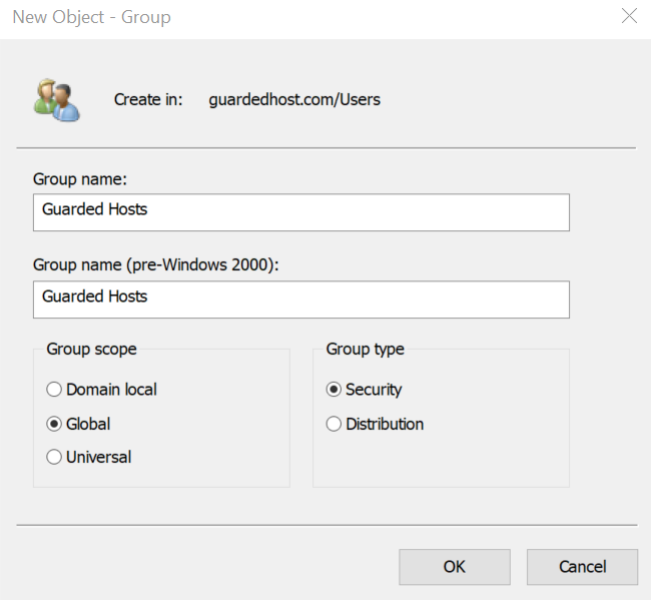
    You can also provide a `.cer` file that contains the public half of the key. Note that the HGS is only used to store and validate the public key. No certificate information is stored on the HGS and neither the certificate chain nor the expiration date is validated by the HGS.

    Open PowerShell as Administrator and run:

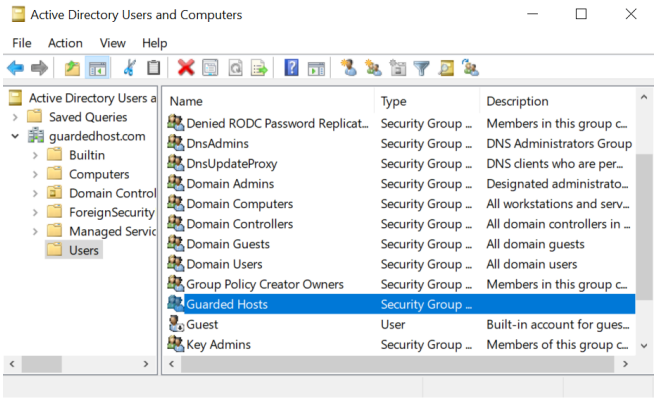
```
> Get-HgsClientHostKey -Path "C:\Users\Administrator\Documents\HostGuardianHst-HostKey.cer"


    Directory: C:\Users\Administrator\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        5/18/2021   3:39 PM            830 HostGuardianHst-HostKey.cer
```

    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.



The security group is created. For example:



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

```
> Get-ADGroup "Guarded Hosts"

DistinguishedName : CN=Guarded Hosts,CN=Users,DC=guardedhost,DC=com
GroupCategory     : 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
----          ----------
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:

```
>  Add-HgsAttestationHostKey -Name HostGuardianHst-HostKey -Path
"C:\Users\Administrator\Documents\HostGuardianHst-HostKey.cer"

Name                    PublicKey
----                    ---------
HostGuardianHst-HostKey System.Security.Cryptography.X509Certificates.PublicKey
```

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 -AttestationServerUrl 'http://hgs.hgs.com/Attestation'-KeyProtectionServerUrl
'http://hgs.hgs.com/KeyProtection'

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 *User Guide* 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.entrust.com. [NOTE] Access to the Entrust Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.
nShield Edge only 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.

Problem	Cause	Solution
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 `unsupported driver` 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:

```
# This is the cardlist file, which contains the serial numbers of any
# Remote Administration Ready Smartcards that a system administrator
# has permitted to be used.
These serial numbers are printed on the
# face of the smartcards
# Examples of valid 16 digit serial numbers:
# XXXXXXXX-XXXXXXXX
# XXXXXXXXXXXXXXXX
# XXXX-XXXX-XXXX-XXXX
# To permit any cards presented to be used:
# *
# The default configuration file has no cards listed, this means
# that all cards will be rejected by default.
*
```