Microsoft Internet Information Services

nShield® HSM Integration Guide

2025-08-06

Member of
Microsoft Intelligent Security Association

Microsoft Security

Table of Contents

Chapter 1. Introduction

Microsoft Internet Information Services (IIS) for Windows Server is a Web server application. Entrust nShield Hardware Security Modules (HSMs) integrate with IIS to provide key protection with FIPS-certified hardware. Integration of the nShield HSM with IIS provides the following benefits:

- Uses hardware validated to the FIPS 140-2 and FIPS 140-3 standards.
- Enables secure storage of the IIS keys.

1.1. Product configuration

Entrust has successfully tested the nShield HSM integration with IIS in the following configuration:

Product	Version
Operating System	Windows 2025 Server
IIS version	10.0

1.2. Supported nShield hardware and software versions

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

Product	Security World Software	Firmware	Netimage
nShield 5c	13.6.11	13.2.4 (FIPS 140-3 certified)	13.6.11
Connect XC	13.6.11	12.72.1 (FIPS 140-2 certified)	13.6.7

1.3. Supported nShield features

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

Feature	Support
Module-Only key	Yes

Feature	Support
OCS cards	Yes [1]
Softcards	No
nSaaS	Yes

[1] OCS without a passphrase and 1/N quorum must be used.

1.4. Requirements

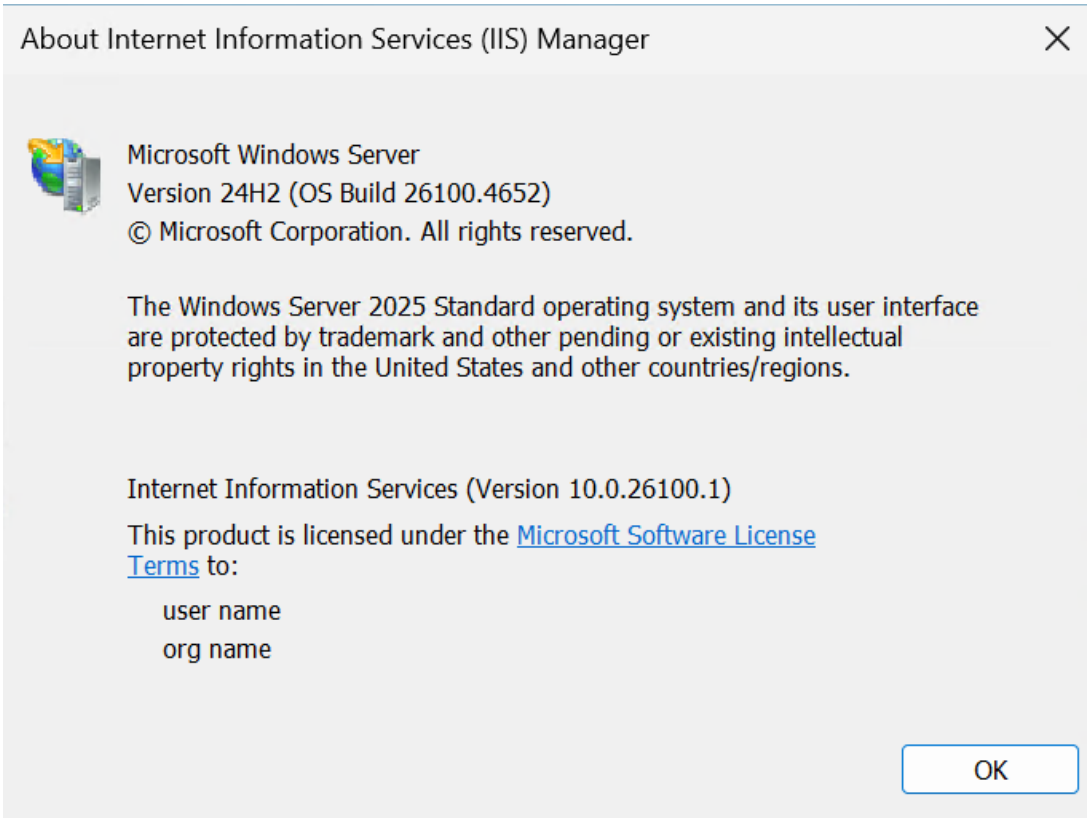
- Knowledge of your organization Certificate Practices Statement and a Security Policy / Procedure in place covering administration of the HSM.
- Access to the Entrust TrustedCare Portal.
- An Entrust nShield HSM.
- A dedicated Windows server.
- Network environment with usable ports 9004 and 9005 for the HSM.

Familiarize yourself with the nShield Documentation.

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

Chapter 2. Deploy and configure Microsoft IIS

IIS was deployed on a dedicated Windows server. The deployment was done using the server manager, accepting all the defaults.



Chapter 3. Deploy and configure the Entrust nShield HSM

All steps below are performed in the server running IIS.

3.1. Install the Entrust nShield HSM

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

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

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

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

1. Install the Security World software. For detailed instructions see the nShield Security World Software v13.6.11 Installation Guide.
2. Add the Security World utilities path to the system path. This path is typically `C:\Program Files\nCipher\nfast\bin`.
3. Open the firewall port 9004 for the HSM connections.
4. If using remote administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).
5. Inform the HSM of the client's location. In this integration the client is the IIS server. For instructions, see Configuring the nShield HSM to use the client. If it's a high-availability setup, repeat the client configuration for each HSM.
6. Enroll the IIS server as a client of the HSM. For instructions, see Configuring client computers to use the nShield HSM. If it's a high-availability setup, repeat the enrolment for each HSM.
7. Open a command window and run the following to confirm the HSM is **operational**:

```
>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        7852-268D-3BF9
```

```
 mode                operational
...
Module #1:
 enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        5F08-02E0-D947
 mode                 operational
 ...
```

8. Create your Security World if one does not already exist or copy an existing one. Follow your organization's security policy for this. For more information see Create a new Security World.

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

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

```
>nfkminfo
World
 generation  2
 state       0x3737000c Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
 Module #2
 generation 2
 state      0x2 Usable
 ...
```

3.3. Select the protection method

IIS binding is only possible with:

- OCS protection
- Module protection.

Typically, an organization's security policies dictate the use of one or the other.

- Operator Cards Set (OCS) are smartcards that are presented to the physical smartcard reader of an HSM. For more information on OCS use, properties, and K-of-N values, see Operator Card Sets (OCS).
- Module protection has no passphrase.

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

Depending on the protection method selected, you may need to define some environment

variables. You have the option to set these environment variables with the Windows `set` command, or edit file `C:\Program Files\nCipher\nfast\cknfastrc`. As reference, all environment variables are listed in nShield PKCS #11 library environment variables.

Enable Module protection:

```
>set CKNFAST_FAKE_ACCELERATOR_LOGIN=1
```

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

```
# Enable Module protection
CKNFAST_FAKE_ACCELERATOR_LOGIN=1

# OCS Preload file location and card set state
NFAST_NFKM_TOKENSFILE="C:\Program Files\nCipher\nfast\preloadtoken"
CKNFAST_NONREMOVABLE=1
```

3.4. Create the OCS

Due to limitations of IIS itself, no GUI prompts (even via nShield Service Agent) can be displayed. Therefore, OCS protection must be passphrase-less and 1/N quorum.

1. Edit file `C:\ProgramData\nCipher\Key Management Data\config\cardlist` adding the serial number of the card(s) to be presented, or the wildcard "*".
2. Open a command window as an administrator.
3. Run the `createocs` command as described below, entering a blank passphrase at the prompt.

   Follow your organization's security policy for the values K/N. Use the same passphrase for all the OCS cards in the set (one for each person with access privilege, plus the spares). In this example note that `slot 2`, remote via a TVD, is used to present the card.

IIS binding requires K = 1 whereas N can be up to, but not exceeding, 64.

After an OCS card set has been created, the cards cannot be duplicated. You may want to create extras in case of a card failure or a lost card.

The preload utility loads OCS onto the HSM. This feature makes the OCS available for use after been physically removed from the HSM for safe storage or other reasons. Add the **-p** (persistent) option to

> the command below to have authentication after the OCS card has been removed from the HSM front panel slot, or from the TVD.

```
> createocs -m1 -s2 -N testOCS -Q 1/1

FIPS 140-2 level 3 auth obtained.

Creating Cardset:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: Admin Card #1
 Module 1 slot 2: empty
 Module 1 slot 3: empty
 Module 1 slot 2: blank cardSteps:

 Module 1 slot 2:- passphrase specified - writing card
Card writing complete.

cardset created; hkltu = a165a26f929841fe9ff2acdf4bb6141c1f1a2eed
```

The authentication provided by the OCS as shown in the command line above is non-persistent and only available while the OCS card is inserted in the HSM front panel slot, or the TVD.

4. Verify the OCS created:

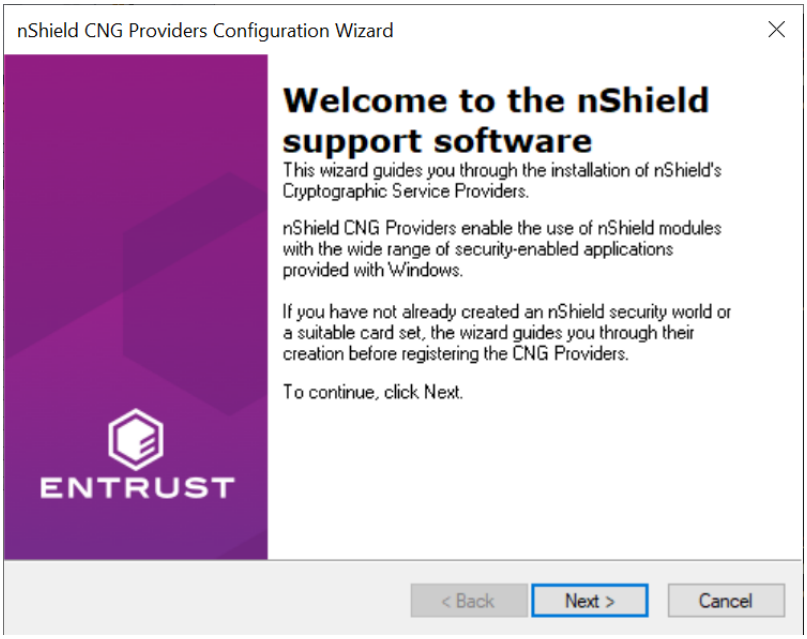
```
>nfkminfo -c
Cardset list - 1 cardsets:  (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
 Operator logical token hash               k/n timeout  name
 7aaf758bc6790206198ea5218040d4faa09f035f  1/5  none-NL testOCSnopassphrase
```

The `rocs` utility also shows the OCS created:

```
>rocs
'rocs' key recovery tool
Useful commands: 'help', 'help intro', 'quit'.
rocs> list cardset
No. Name                    Keys (recov) Sharing
  1 testOCSnopassphrase     0 (0)        1 of 5
rocs> quit
```

Chapter 4. Install and register the CNG provider

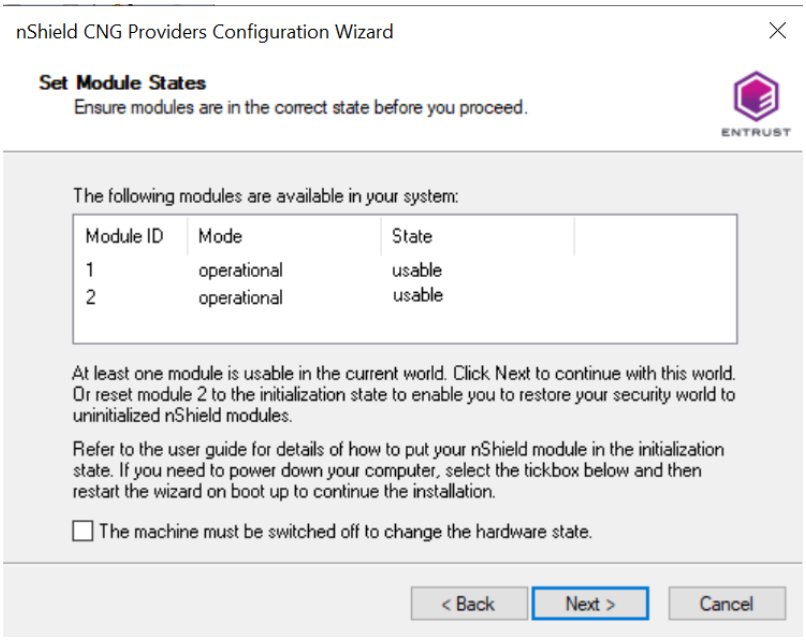
1. Select **Start** > **Entrust** > **CNG configuration wizard**.
2. Select **Next** on the **Welcome** window.



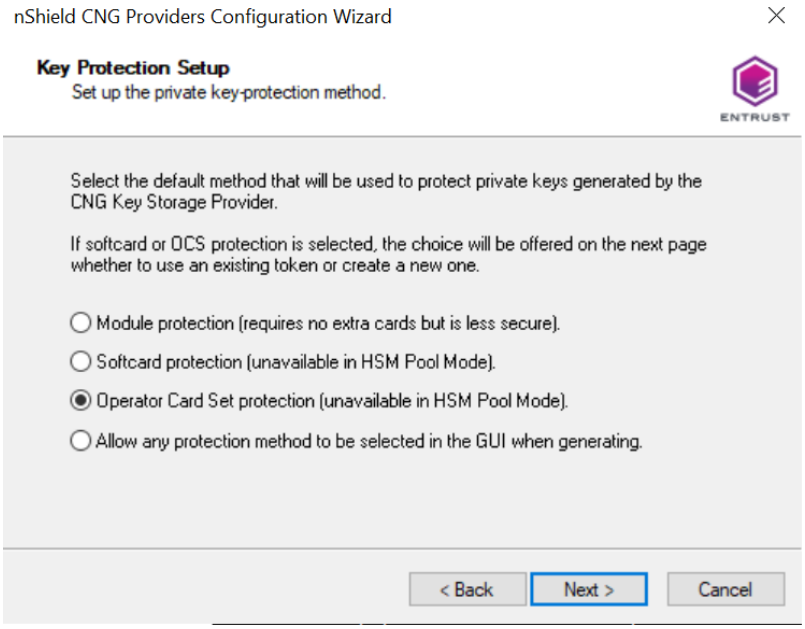
3. Select **Next** on the **Enable HSM Pool Mode** window, leaving **Enable HSM Mode for CNG Providers** un-checked.

> 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 `Key Management Data\local` directory.

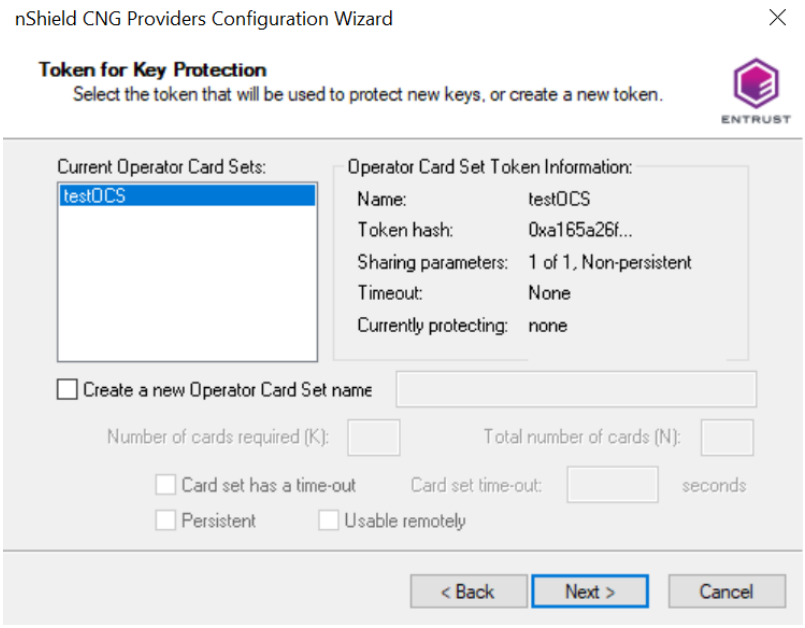
4. On the **Initial setup** window, select **Use existing security world**. Then select **Next**.
5. On the **Set Module States** window, select the HSM (Module) if more than one is available. Then select **Next**.



6. On **Key Protection Setup** window, select **Operator Card Set protection**. Then select **Next**.



7. On the **Token for Key Protection** window, choose from the **Current Operator Card Sets** list created in Create the OCS. Then select **Next** and **Finish**.

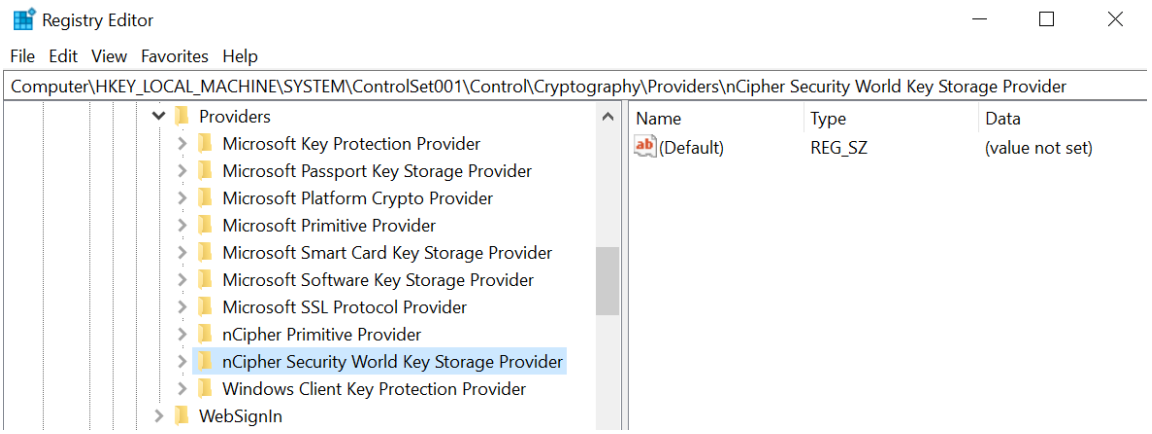


8. Verify the provider with the following commands.

```
>certutil -csplist | findstr nCipher
Provider Name: nCipher Security World Key Storage Provider

>cnglist.exe --list-providers | findstr nCipher
nCipher Primitive Provider
nCipher Security World Key Storage Provider
```

9. Verify the provider in the Windows Registry.

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Cryptography\Providers\nCipherSecurityWorldKeyStorageProvider
```



Chapter 5. Integrate a new IIS deployment with the nShield HSM

This section describes how to integrate a new IIS server installation with an nShield HSM.

5.1. Create a certificate request

IIS Manager does not support the creation of certificate requests protected by CNG Keys. These must be created using the Microsoft command line utilities on Windows PowerShell.

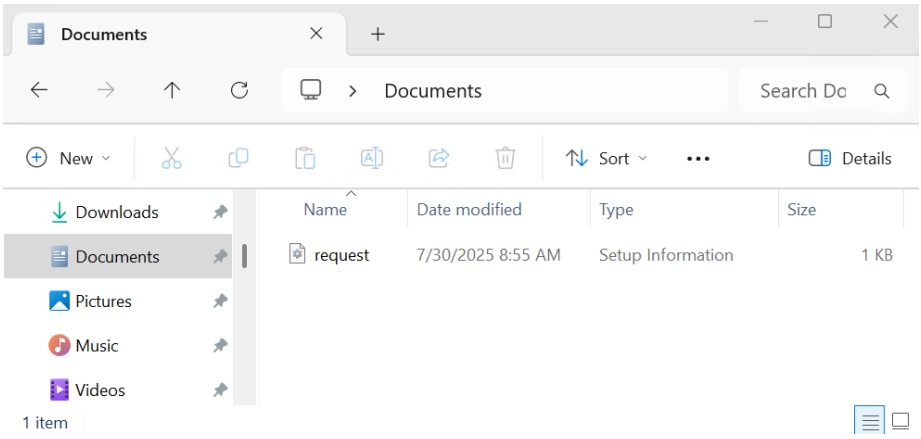
1. Verify the **nCipher Primitive Provider** and **nCipher Security World Key Storage Provider** are available. Otherwise, see section Install and register the CNG provider.

   ```
   >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
   ```

2. Create a `request.inf` file for an SSL certificate linked to a 2048 RSA key protected by the HSM. Notice the **ProvideName** set to **nCipher Security World Key Storage Provider**.

   For example:

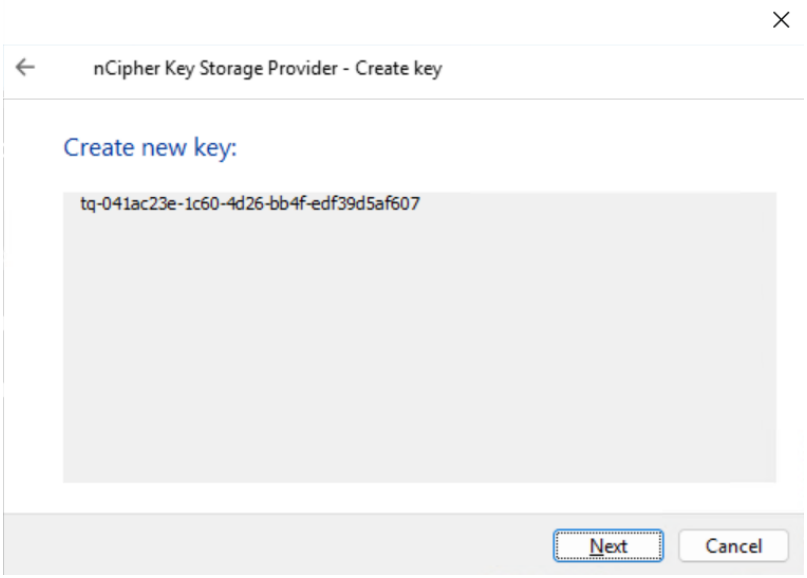
   ```
   [Version]
   Signature= "$Windows NT$"
   [NewRequest]
   Subject = "CN=interop.local,C=US,ST=Florida,L=Sunrise,O=InteropLocal,OU=WebServer"
   HashAlgorithm = SHA256
   KeyAlgorithm = RSA
   KeyLength = 2048
   ProviderName = "nCipher Security World Key Storage Provider"
   KeyUsage = 0xf0
   MachineKeySet = True
   [EnhancedKeyUsageExtension]
   OID = 1.3.6.1.5.5.7.3.1
   ```



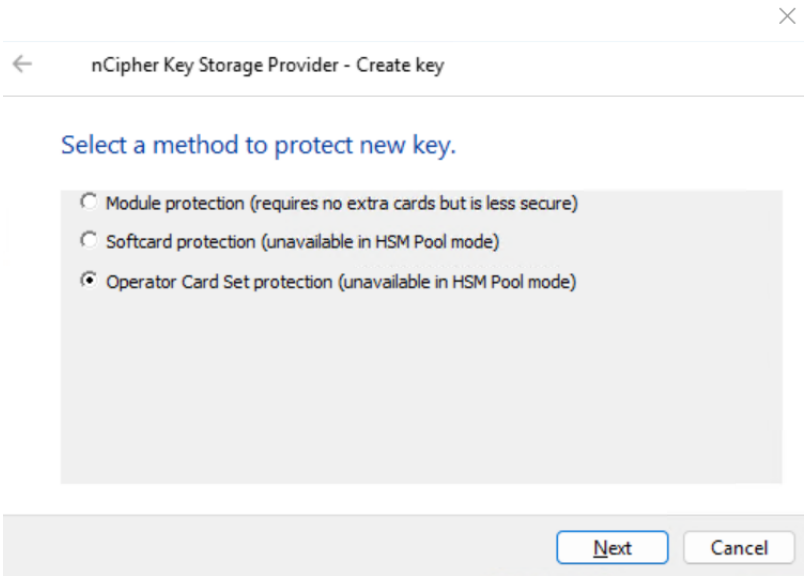
3. Run the following command to create the certificate request.

```
> certreq.exe -new request.inf IISCertRequest.csr
```

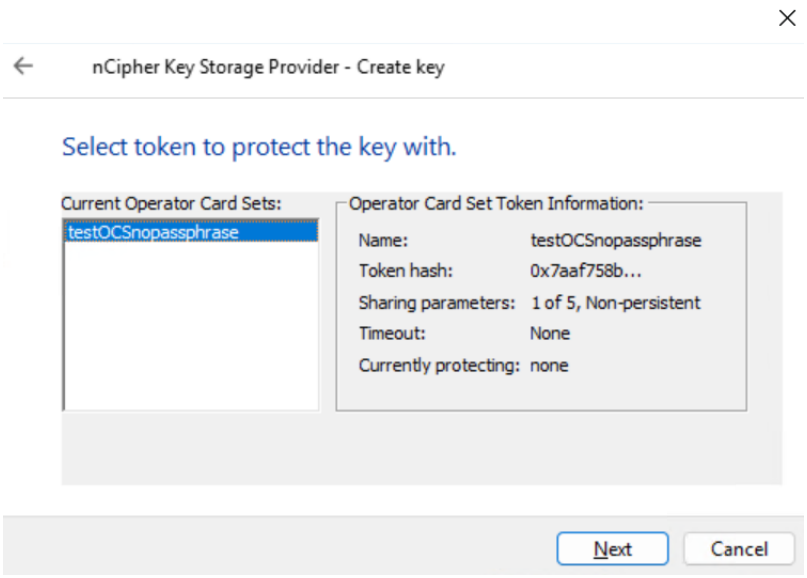
4. In the **nCipher Key Storage Provider - Create Key** pop-up window, select **Next**.



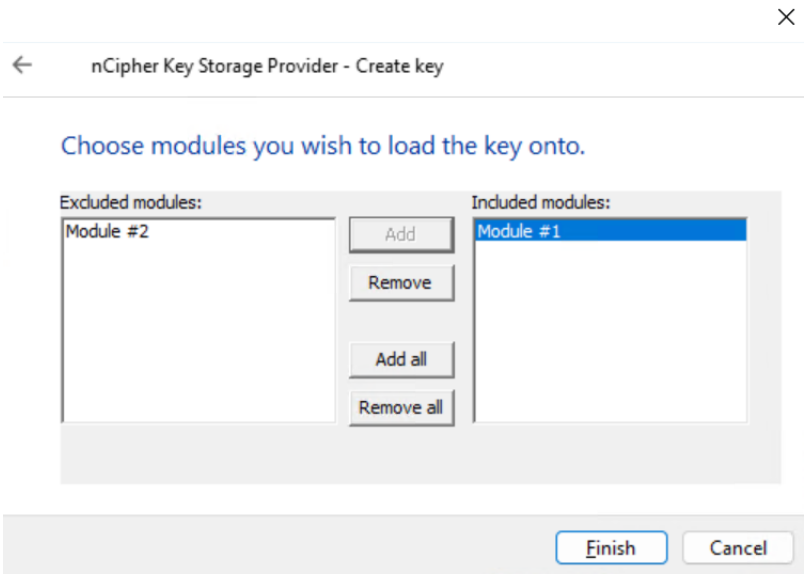
5. Select **Operator Card Set protection**. Then select **Next**.



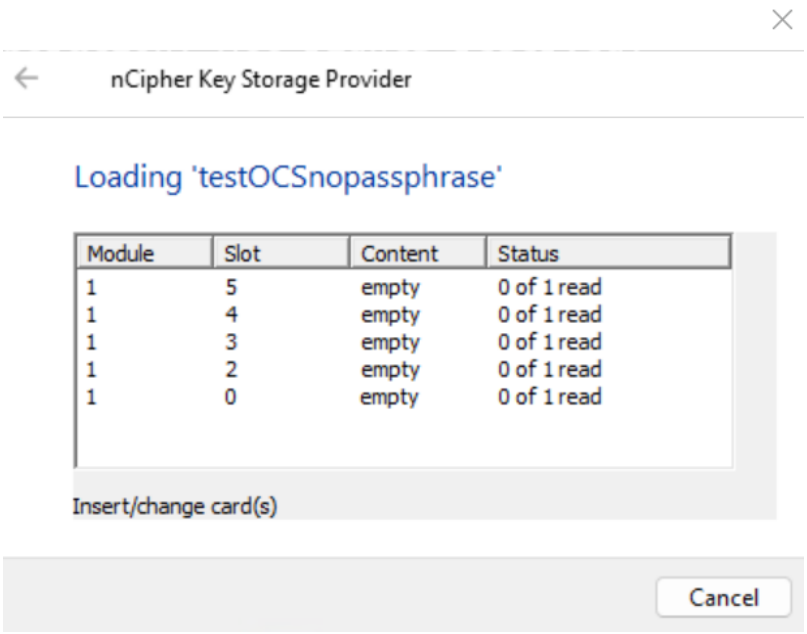
6. Chose the OCS. Then select **Next**.



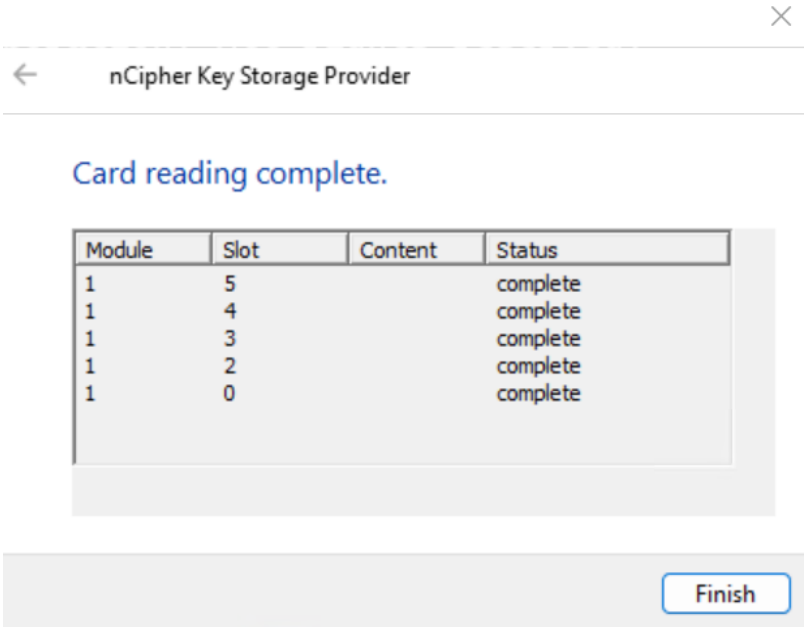
7. Chose the HSM. Then select **Finish**.



8. Present the OCS to the HSM.



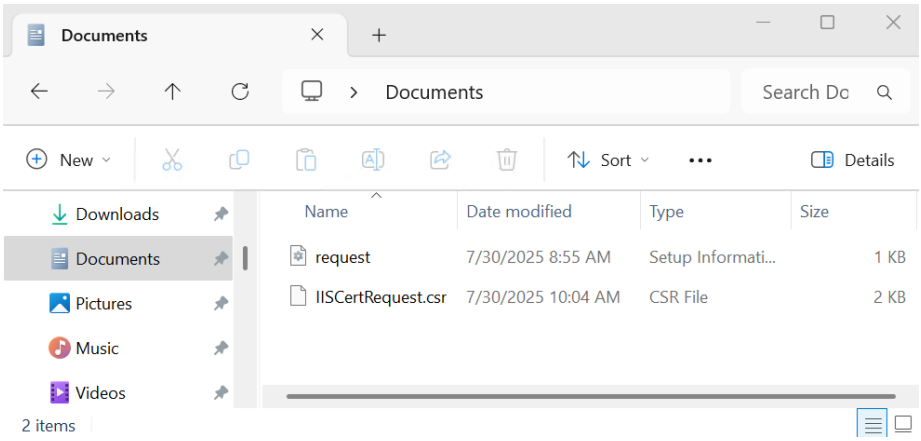
9. In the **Card reading complete.** window, select **Finish**.



10. Notice the command completed in the CLI.

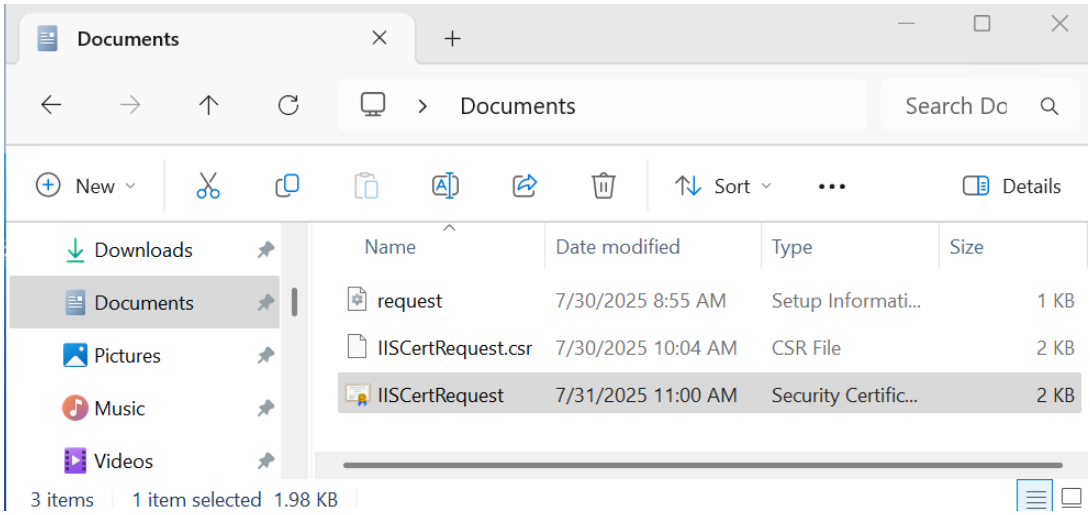
```
>certreq.exe -new request.inf IISCertRequest.csr

CertReq: Request Created
```

11. Notice the `csr` file created.



5.2. Sign the certificate request

Submit the CSR file for signature to your organization's CA. For this integration a local two-tier PKI infrastructure was used for signing. The signed certificate file is `IISCertRequest.cer`.



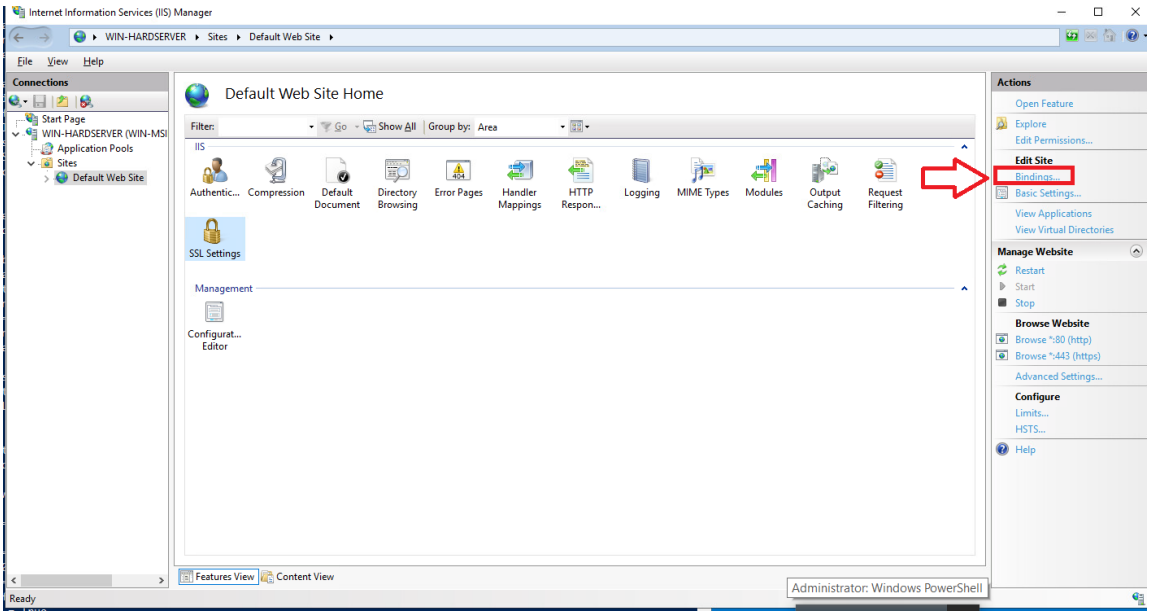
5.3. Install the certificate

Open a command window and run the following to make the signed certificate available for use in IIS.

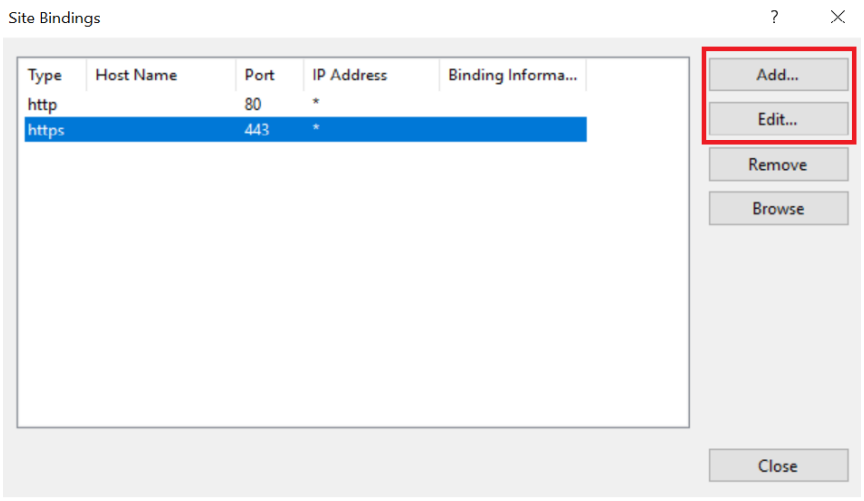
```
>certreq -accept IISCertRequest.cer
Installed Certificate:
  Serial Number: 39000000171fd041e27d84cc65000000000017
  Subject: CN=interop.local, OU=WebServer, O=InteropLocal, L=Sunrise, S=Florida, C=US
  NotBefore: 7/31/2025 10:46 AM
  NotAfter: 7/31/2027 10:46 AM
  Thumbprint: bc504bb69b98ec801d8907b47d0a82b80f6dcd92
```

5.4. Bind the certificate to the IIS server

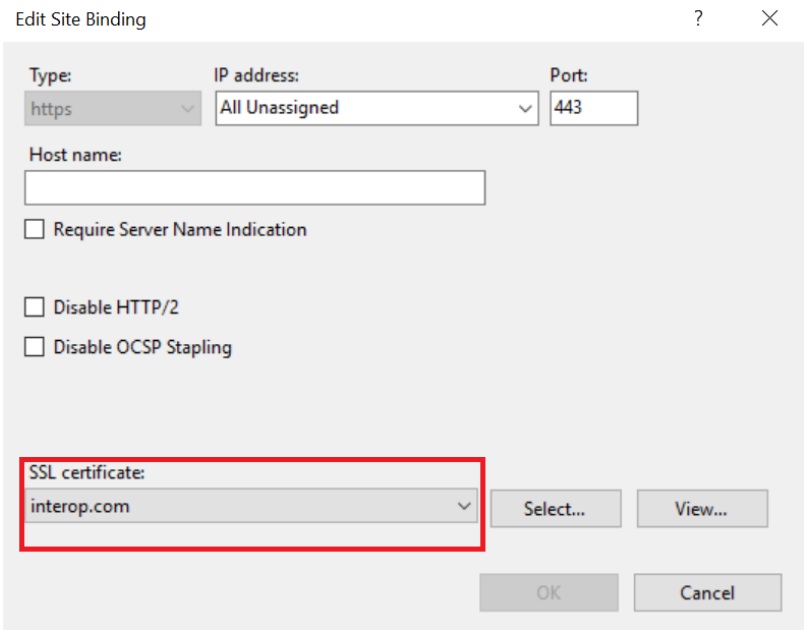
1. Go to **Start** > **Internet Information Service Manager**.
2. Select the hostname, then double-click **Server Certificates** and verify the certificate you accepted in the previous step is listed.
3. Under **Sites** on the left-hand side of the IIS Manager screen, select **Default website**.
4. Select **Bindings** link on the right-hand side of the IIS Manager.



5. In the **Site Bindings** window, if the **https** protocol is not listed add it now. To do this, select **Add**, set the protocol as **https** and select the required certificate from the list.



6. Select the **https** protocol, select **Edit**, and then select the certificate from the list:



7. Select **OK** to complete the certificate binding for SSL connection.
8. Select **Close** on the **Site Bindings** screen.
9. Restart the IIS server.

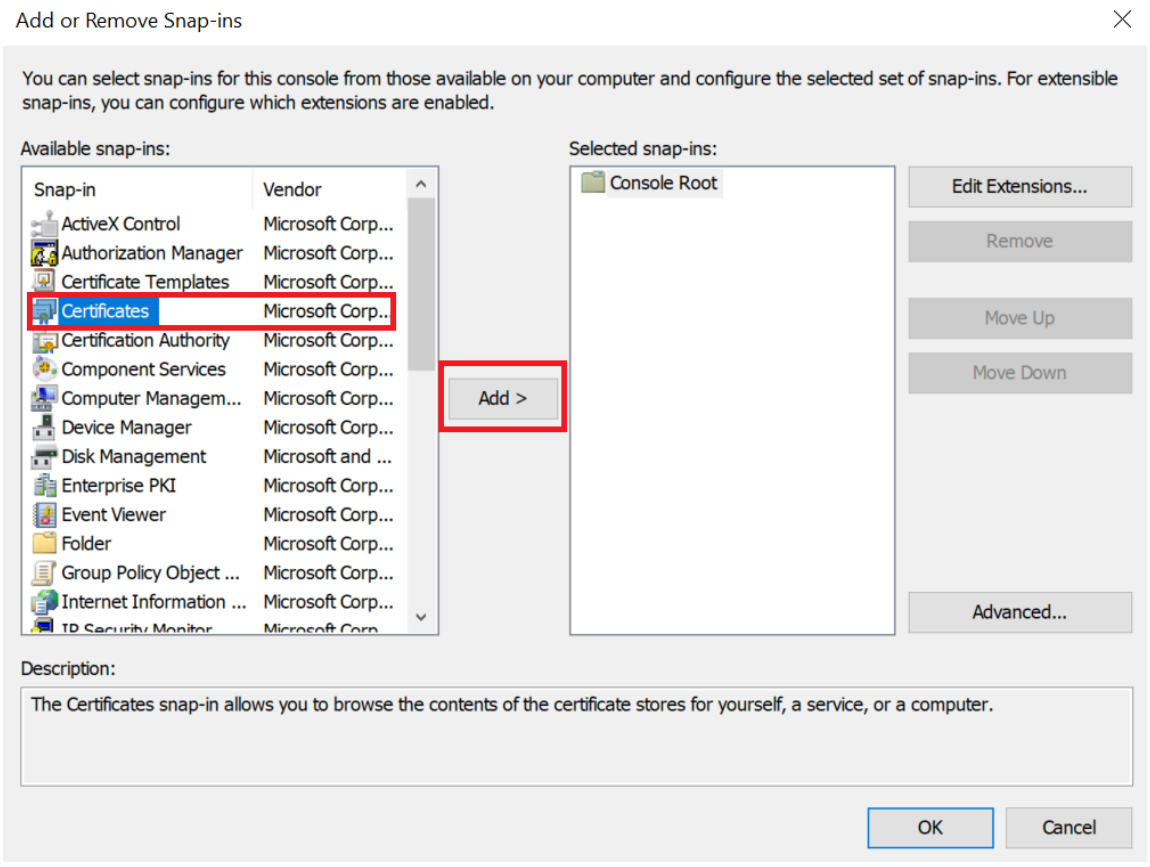
Chapter 6. Integrate an existing IIS deployment with the nShield HSM

This section describes how to integrate an existing IIS server installation with an nShield HSM. It is assumed the existing IIS server has a software-protected certificate and private key, and that you have a new valid **Origin Server** certificate.

6.1. Export the software-protected certificate

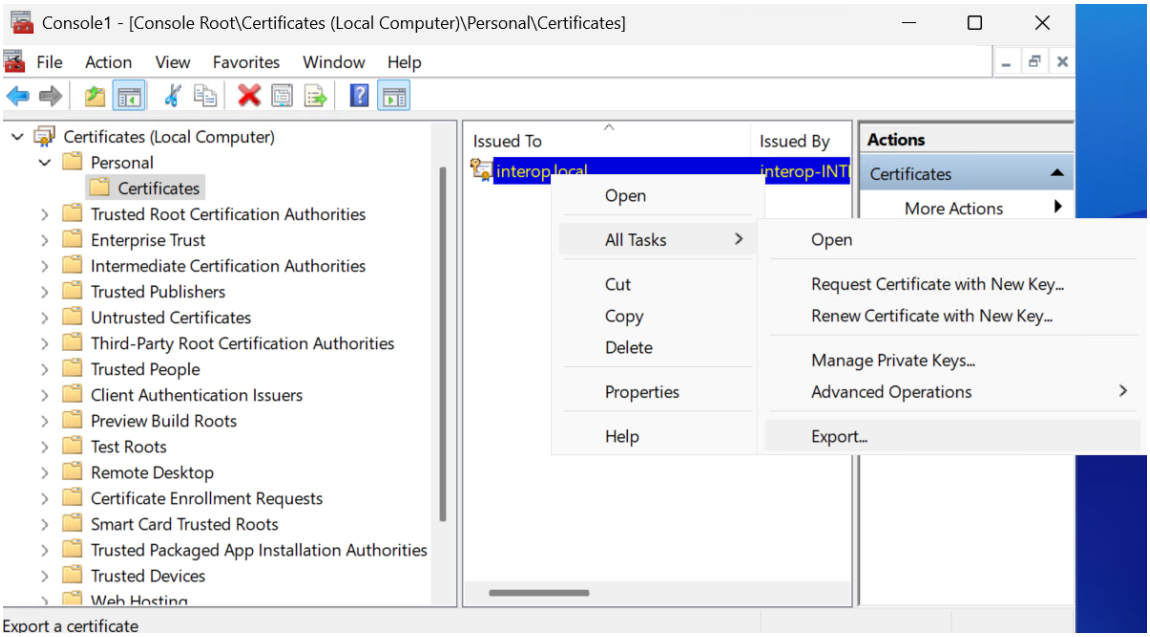
Export the original certificate from the personal folder in the local computer's certificate store. Then delete the certificate from the store.

1. Type **MMC** in the Windows search text box and select **OK**.
2. On the Console window, select **File** > **Add/Remove Snap-in**.
3. Select **Certificates** from **Available Standalone Snap-ins**. Then select **Add**.

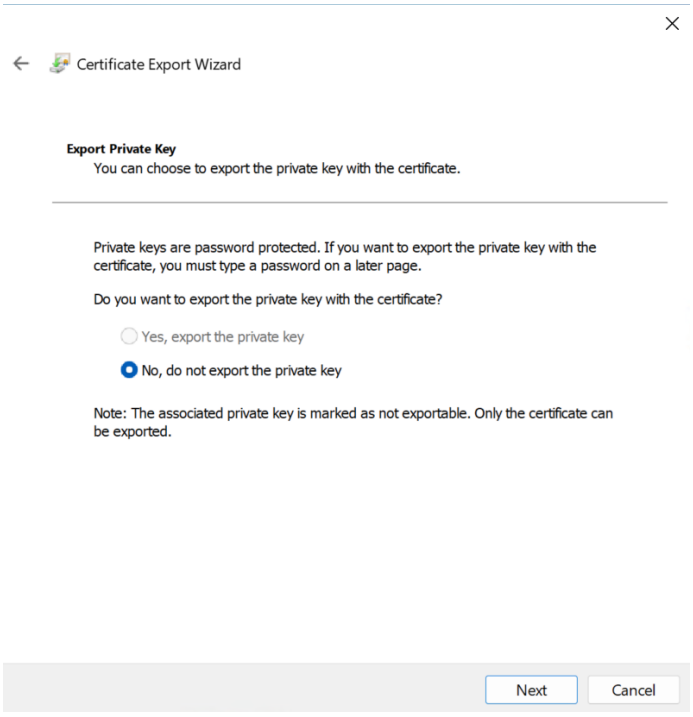


4. On the **Certificates snap-in** window, select **Computer account**. Then select **Next**.
5. On the **Select Computer** window, select **Local computer**. Then select **Finish** and **OK**.
6. Navigate to **Certificates (Local Computer)** > **Personal** > **Certificates**.

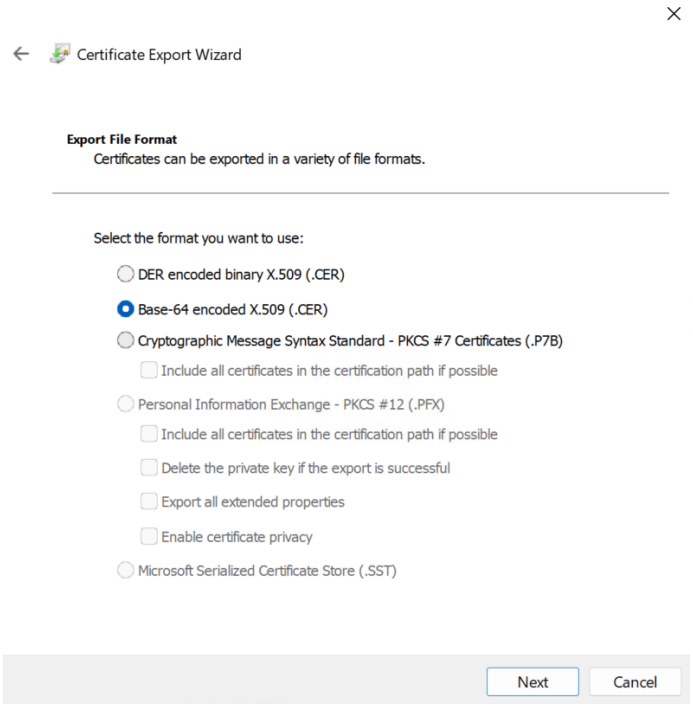
7. Right-select the certificate file and select **All Tasks** > **Export**.



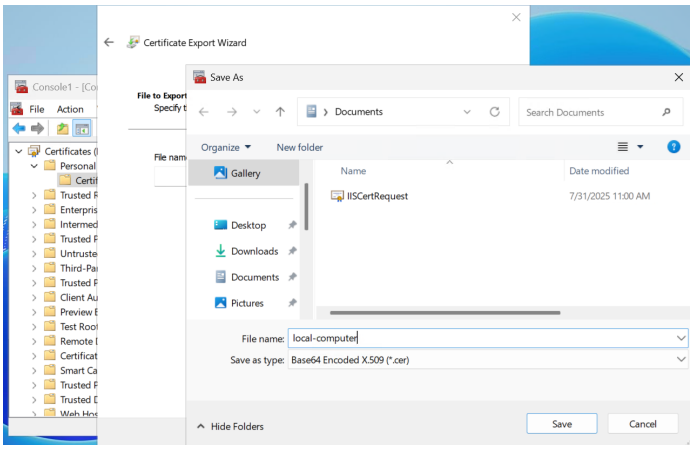
8. On the **Welcome to the Certificate Export Wizard** window, select **Next**.
9. On the **Export Private Key** window, select **No, do not export the private key**. Then select **Next**.



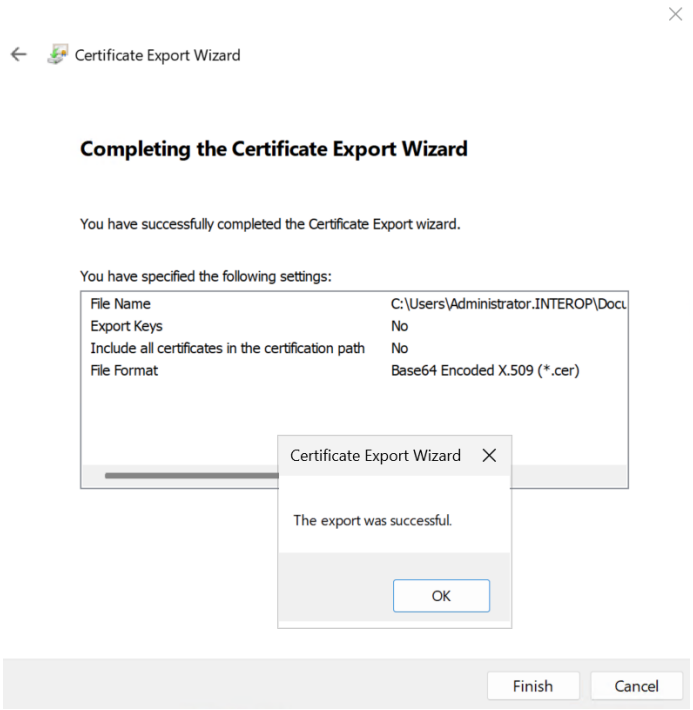
10. On the **Export File Format** window, select **Base-64 encoded X.509 (.Cer)** and select **Next**.



11. On the **File to Export** window, select an absolute path and filename to save the exported certificate. Then select **Next** twice.



12. On the **Completing the Certificate Export Wizard** window, select **Finish** and **OK**.

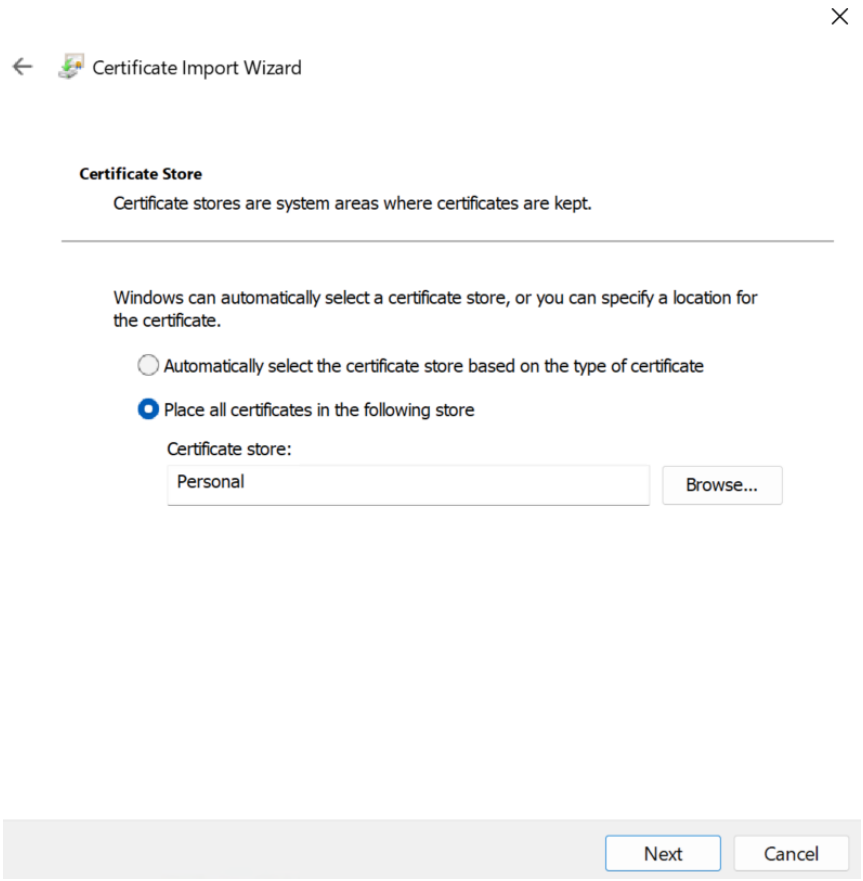


13. After exporting the certificate, delete the certificate from the **Personal** certificate store.

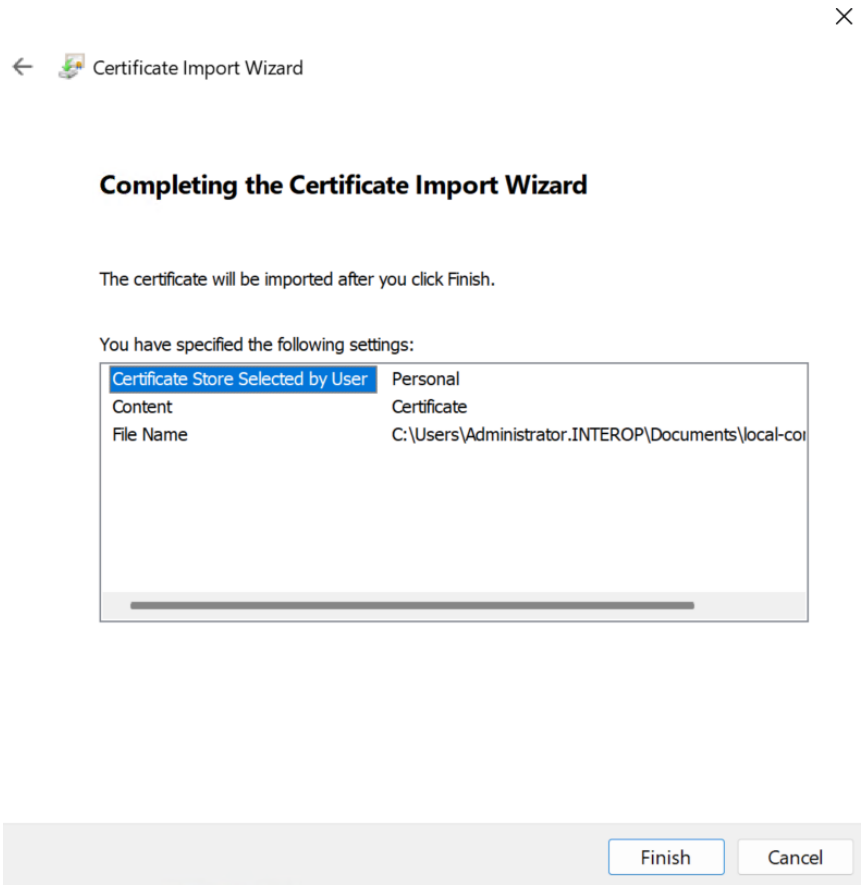
6.2. Import new certificate into the certificate store

Import a new valid **Origin Server** certificate and assign it a private key protected by the nShield HSM.

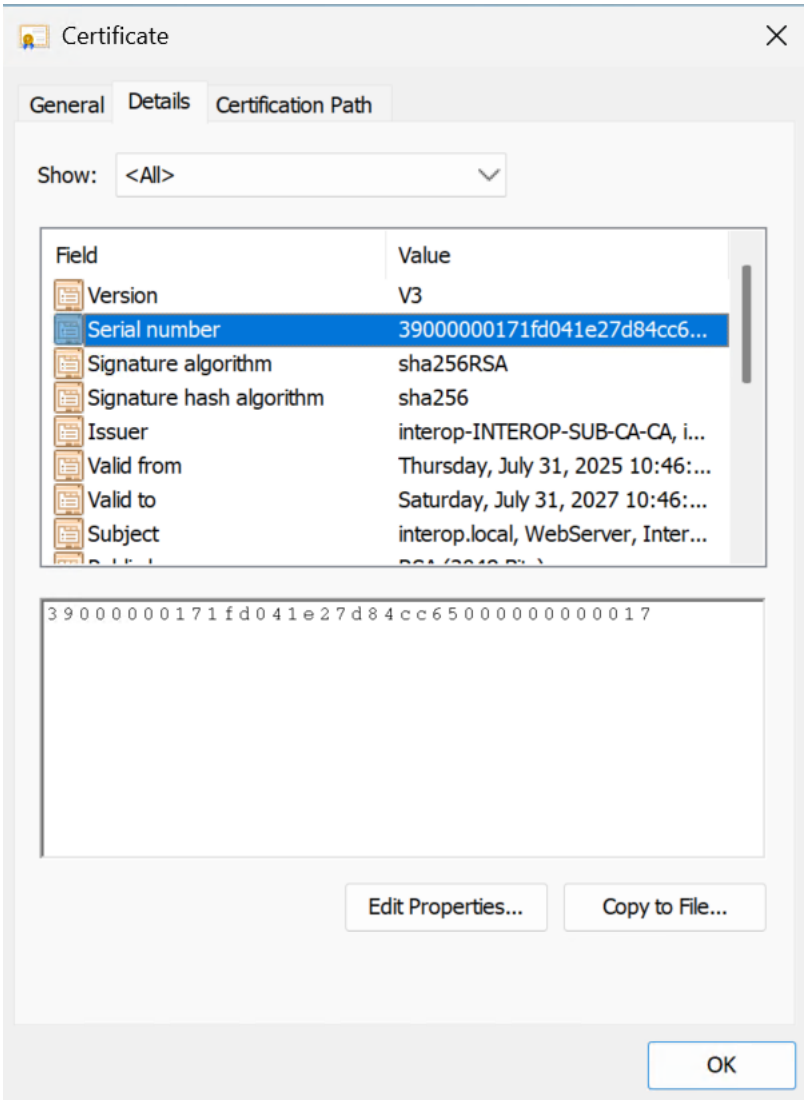
1. Type **MMC** in the Windows search text box and select **OK**.
2. On the Console window, select **File** > **Add/Remove Snap-in**.
3. Select **Certificates** from **Available Standalone Snap-ins**. Then select **Add**.
4. On the **Certificates snap-in** window, select **Computer account**. Then select **Next**.
5. On the **Select Computer** window, select **Local computer**. Then select **Finish** and **OK**.
6. Navigate to **Certificates (Local Computer)** > **Personal** > **Certificates**.
7. Right-select the certificate folder and select **All Tasks** > **Import**.
8. On the **Welcome to the Certificate Import Wizard** window, select **Next**.
9. Navigate to the location of the certificate from the **Origin Server** and select it. Then select **Next**.
10. On the **Certificate Store** window, select **Place all certificates in the following store**. Enter **Personal** in the text box. Then select **Next**



11. On the **Completing the Certificate Import Wizard** window, select **Finish**. Select **Next** and **OK**.



12. On the **Personal** store locate the certificate, right-select and select **Open**.
13. On the **Certificate** window, select the **Details** tab.
14. Locate the serial number of the certificate.



15. Run the following command from a Windows terminal:

```
>certutil -f -csp "nCipher Security World Key Storage Provider" -repairstore my <serial number of
certificate>

>certutil -f -csp "nCipher Security World Key Storage Provider" -repairstore my
39000000171fd041e27d84cc65000000000017
my "Personal"
================ Certificate 0 ================
Serial Number: 39000000171fd041e27d84cc65000000000017
Issuer: CN=interop-INTEROP-SUB-CA-CA, DC=interop, DC=local
 NotBefore: 7/31/2025 10:46 AM
 NotAfter: 7/31/2027 10:46 AM
Subject: CN=interop.local, OU=WebServer, O=InteropLocal, L=Sunrise, S=Florida, C=US
Certificate Template Name (Certificate Type): WebServer
Non-root Certificate
Template: WebServer, Web Server
Cert Hash(sha1): bc504bb69b98ec801d8907b47d0a82b80f6dcd92
  Key Container = tq-041ac23e-1c60-4d26-bb4f-edf39d5af607
  Provider = nCipher Security World Key Storage Provider
Private key is NOT exportable
ERROR: Could not verify certificate public key against private key
nCipher Security World Key Storage Provider: KeySpec=0
AES256+RSAES_OAEP(RSA:CNG) test passed
```

```
CertUtil: -repairstore command completed successfully.
```

6.3. Bind the certificate to the IIS server

1. Open the IIS Manager from **Start** > **Internet Information Services (IIS) Manager**.
2. Under **Sites** on the left-hand side of the **IIS Manager** window, select the applicable web site.
3. On the right-hand side of the **IIS Manager** window, select **Bindings**.
4. On the **Site Bindings** screen, select **Add**.
5. Select the protocol **https**.
6. Select the certificate from the drop-down list.
7. To complete the certificate binding for SSL connection, select **OK** and **Close**.

Chapter 7. Appendix

7.1. Import a Microsoft CAPI key into the nCipher Security World key storage provider

1. Navigate to the `C:\Program Files\nCipher\nfast\bin` folder and run `cngimport.exe` in the command prompt:

   ```
   cngimport -m -M -k "MS CAPI key"  "imp_key_name"
   ```

   The Microsoft CNG key is in the `C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys` folder. For example:

   ```
   cngimport -m -M -k,"48753e97af4e829f_b2885b-321a-42b9-9122-81d377654436" "Importedkeyname"
   ```

2. To check the success of the import, list the keys in the Security World in the command prompt:

   ```
   cnglist --list-key
   ```

Chapter 8. Additional resources and related products

8.1. nShield Connect

8.2. nShield as a Service

8.3. Entrust products

8.4. nShield product documentation