Member of
Microsoft Intelligent
Security Association

Microsoft Security

Microsoft Internet Information Services and Windows Server 2019

nShield® HSM Integration Guide

2023-12-12

Table of Contents

Chapter 1. Introduction

Microsoft Internet Information Services (IIS) for Windows Server is a Web server application. nShield Hardware Security Modules (HSMs) integrate with IIS 10.0 to provide key protection with FIPS-certified hardware. Integration of the nShield HSM with IIS 10.0 provides the following benefits:

- Uses hardware validated to the FIPS 140 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 2019 Server
IIS version	10.0

1.2. Supported nShield hardware and software versions

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

1.2.1. nShield

Product	Security World Software	Firmware	Netimage	OCS	Softcard	Module
nSaaS	13.3.2	12.72.1 (FIPS Certified)	12.80.5	✓		✓
Connect XC	13.3.2	12.72.1 (FIPS Certified)	12.80.5	✓		✓

Product	Security World Software	Firmware	Netimage	OCS	Softcard	Module
nShield 5c	13.3.2	13.3.2 (FIPS Pending)	13.3.2	✓		✓

1.3. Requirements

Before installing the software, Entrust recommends that you familiarize yourself with the IIS documentation and set-up process, and that you have the nShield documentation available. Entrust also recommends that there is an agreed organizational Certificate Practices Statement and a Security Policy/Procedure in place covering administration of the HSM. In particular, these documents should specify the following aspects of HSM administration:

- The number and quorum of Administrator Cards in the Administrator Card Set (ACS) and the policy for managing these cards.
- Whether the application keys are protected by the HSM module key or an Operator Card Set (OCS) protection.
- Whether the Security World should be compliant with FIPS 140 Level 3.
- Key attributes such as the key algorithm, key length and key usage.

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

For more information, see the *User Guide* for the HSM.

Chapter 2. Procedures

Integration procedures include:

- Select the protection method
- Install the nShield HSM
- Install the Security World software and create a Security World
- Create the OCS
- Install and register the CNG provider
- Install IIS
- Create a certificate request
- Get the signed certificate
- Install the certificate
- Integrate an nShield HSM with an existing IIS deployment

2.1. Select the protection method

For this integration, IIS binding is only possible with:

- OCS without a passphrase.
- Module protection.

Follow your organization's security policy to select which one.

2.2. Install the nShield HSM

Install the HSM and Security World software using the instructions in the *Installation Guide* for the HSM. Entrust recommends that you do this before installing and configuring IIS.

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

1. Install the Security World software. For instructions, see the *Installation Guide* and the *User Guide* for the HSM.
2. Add the Security World utilities path `C:\Program Files\nCipher\nfast\bin` to the Windows system path.

3. Open 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 confirm that the HSM is `operational`:

```
C:\Users\Administrator.INTEROP>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        5F08-02E0-D947 6A74-1261-7843
 mode                 operational
 version              12.80.4
...
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        5F08-02E0-D947
 mode                 operational
 version              12.72.1
 ...
```

6. Create your Security World if one does not already exist, or copy an existing one. Follow your organization's security policy for this.
7. Confirm that the Security World is `usable`:

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

2.4. Create the OCS

If using OCS protection, create the OCS now. Follow your organization's security

policy for the value N of K/N. As required, create extra OCS cards, one for each person with access privilege, plus spares.

Administrator Card Set (ACS) authorization is required to create an OCS in FIPS 140 level 3.

After an OCS card set has been created, the cards cannot be duplicated.

1. If using remote administration, ensure the `C:\ProgramData\nCipher\Key Management Data\config\cardlist` file contains the serial number of the card(s) to be presented.
2. Open a command window as administrator.
3. Execute the following command. Follow your organization's security policy for the values K/N. The OCS cards cannot be duplicated after they are created. Do **not** enter a passphrase or password at the prompt, just press **Return**. Notice `slot 4`, remote via a Trusted Verification Device (TVD), is used to present the card. In this example, K=1 and N=1.

```
>createocs -m1 -s4 -N testOCS -Q 1/1

FIPS 140 level 3 auth obtained.

Creating Cardset:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: Admin Card #1
 Module 1 slot 4: blank card
 Module 1 slot 3: unknown card
 Module 1 slot 2: empty
 Module 1 slot 5: empty
 Module 1 slot 4:- no passphrase specified - writing card
Card writing complete.

cardset created; hkltu = 991b6cb36db1adbe317964086273eee97e466123
```

   Add the `-p` (persistent) option to the command above to retain authentication after the OCS card has been removed from the HSM front panel slot, or from the TVD. If using OCS card protection and the non-persistent card configuration, OCS cards must be be inserted in the nShield front panel or always present in the TVD. The authentication provided by the OCS as shown in the command line above is non-persistent and only available for K=1, and while the OCS card is present in the HSM front panel slot, or 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
```

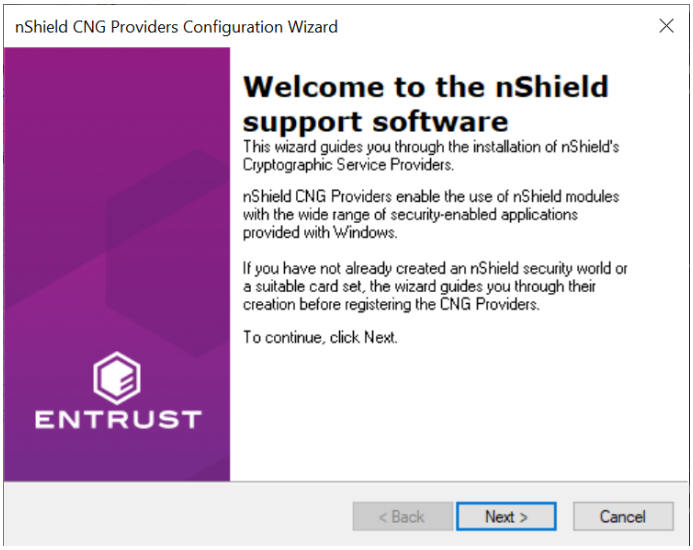
```
991b6cb36db1adbe317964086273eee97e466123  1/1  none-NL testOCS
```

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 testOCS                 0 (0)        1 of 1
rocs> quit
```

2.5. Install and register the CNG provider

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

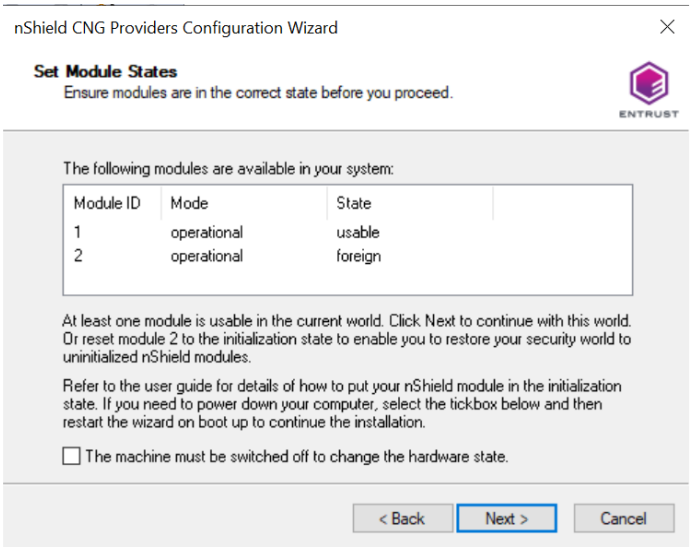


3. Select **Next** on the **Enable HSM Pool Mode** window, leaving **Enable HSM Mode for CNG Providers** un-checked.

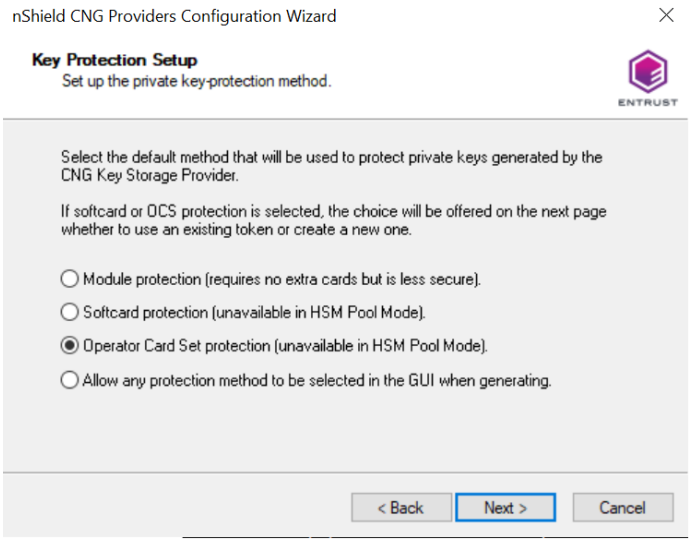
> If you intend to use multiple HSMs in a failover and load-sharing capacity, select **Enable HSM Pool Mode for CNG Providers**. If you do, you can only use module protected keys. Module protection does not provide conventional 1 or 2 factor authentication. Instead, the keys are encrypted and stored as an application key token, also referred to as a Binary Large Object (blob), in the `kmdata/local` directory.

4. Select **Use existing security world** on the **Initial setup** window. Then select **Next**.

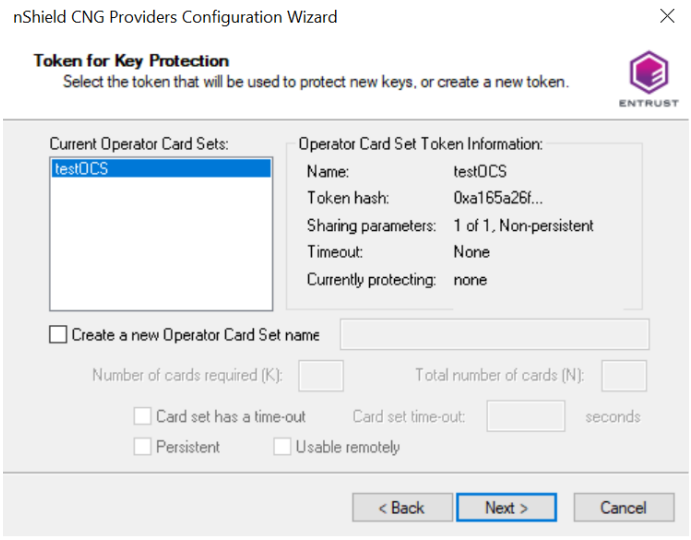
5. Select the HSM (Module) if more than one is available on the **Set Module States** window. Then select **Next**.



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



7. Choose from the **Current Operator Card Sets** or **Current Softcards** list. Notice these were created above. Then select **Next** and **Finish**.



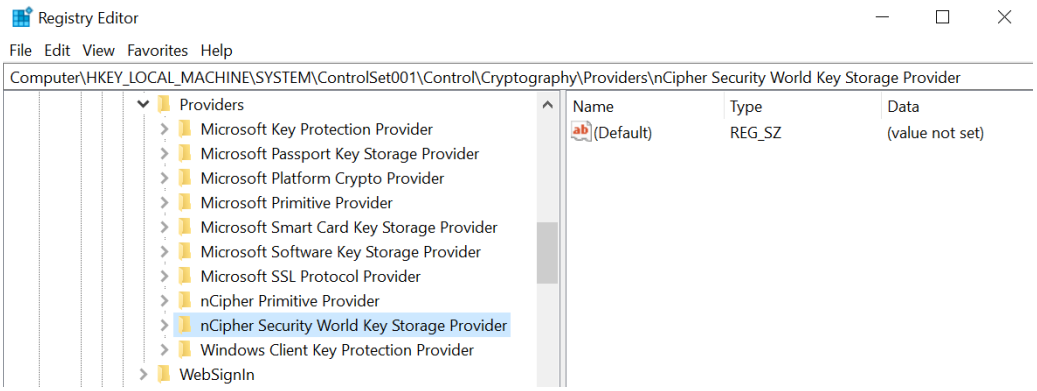
8. Verify the provider with the following commands:

```
>certutil -csplist | findstr nCipher
Provider Name: nCipher DSS Signature Cryptographic Provider
Provider Name: nCipher Enhanced Cryptographic Provider
Provider Name: nCipher Enhanced DSS and Diffie-Hellman Cryptographic Provider
Provider Name: nCipher Enhanced DSS and Diffie-Hellman SChannel Cryptographic Provider
Provider Name: nCipher Enhanced RSA and AES Cryptographic Provider
Provider Name: nCipher Enhanced SChannel Cryptographic Provider
Provider Name: nCipher Signature Cryptographic Provider
Provider Name: nCipher Security World Key Storage Provider

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

9. Check the registry in `CNGRegistry`:

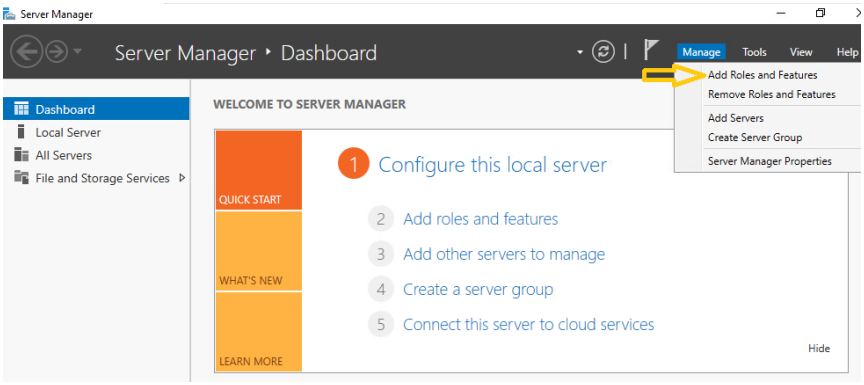
```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Cryptography\Providers\nCipherSecurityWorldKeyStorageProvid
er
```



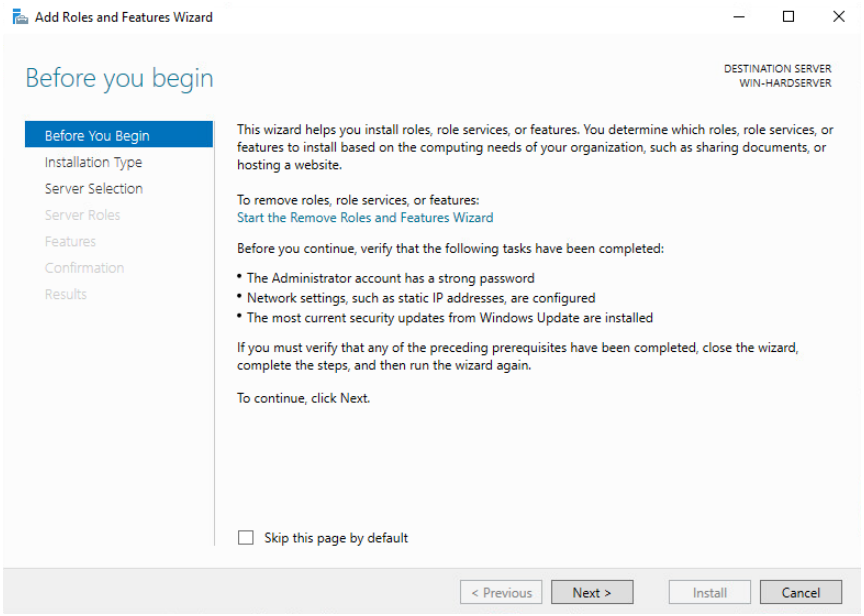
2.6. Install IIS

To install Microsoft Internet Information Services:

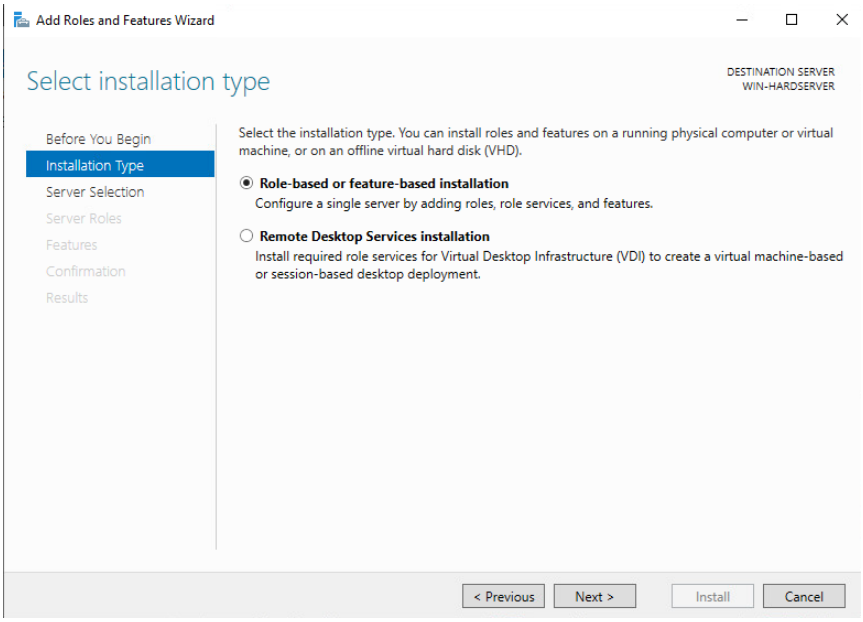
1. Open Server Manager by selecting **Start > Server Manager**.
2. Select **Manage** and then select **Add Roles and Features**.



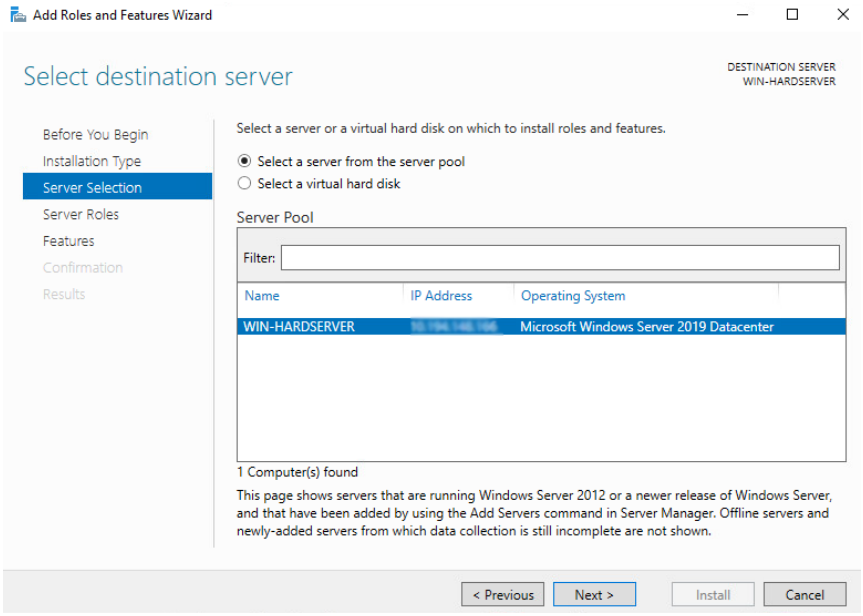
3. On the **Before you begin** screen, select **Next**.



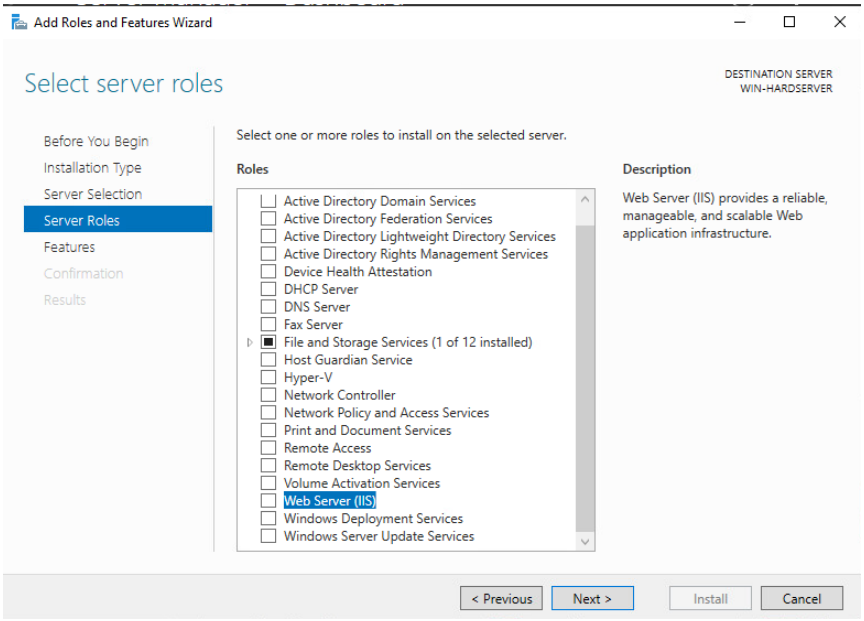
4. On the **Select installation type** screen, ensure the default selection of **Role or Feature Based Installation** is selected and select **Next**.



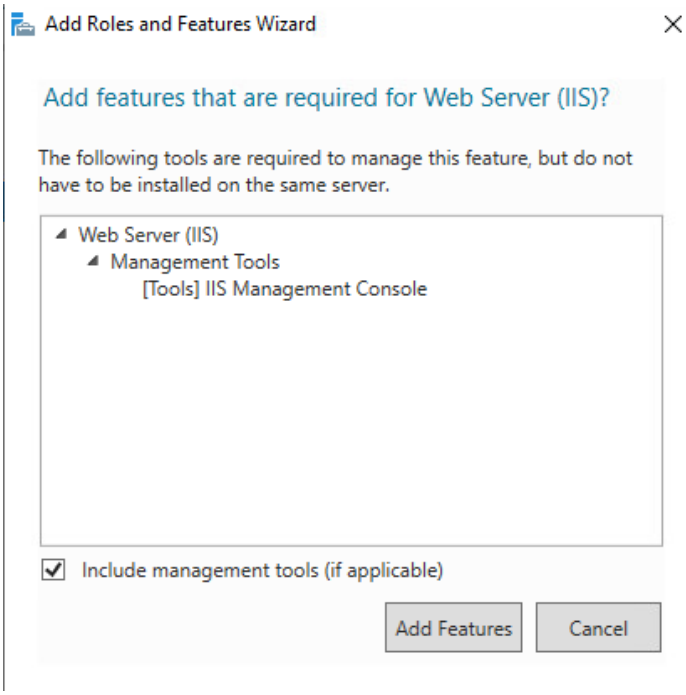
5. On the **Server Selection** screen, select a server from the server pool and select **Next**.



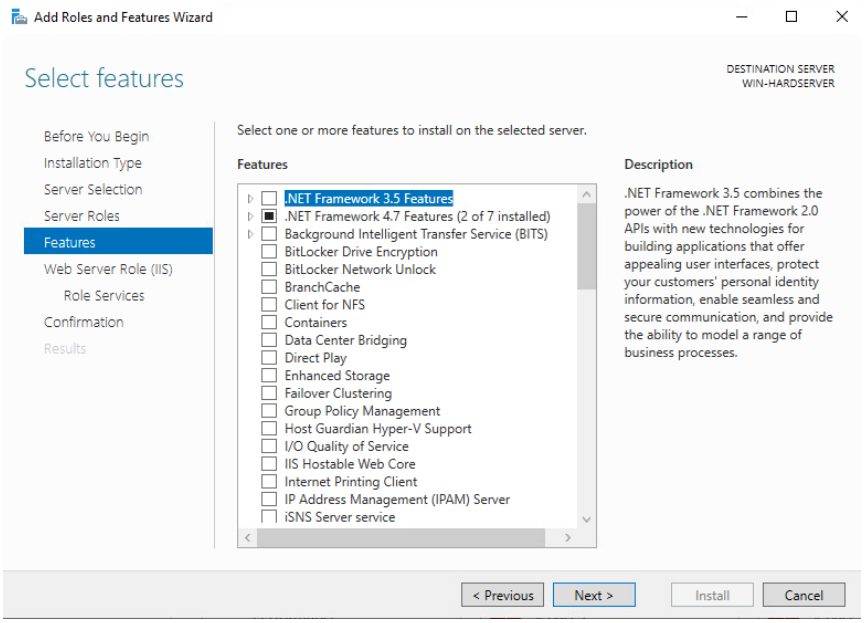
6. On the **Select server roles** screen, select the **Web Server (IIS) Role** and select **Next**



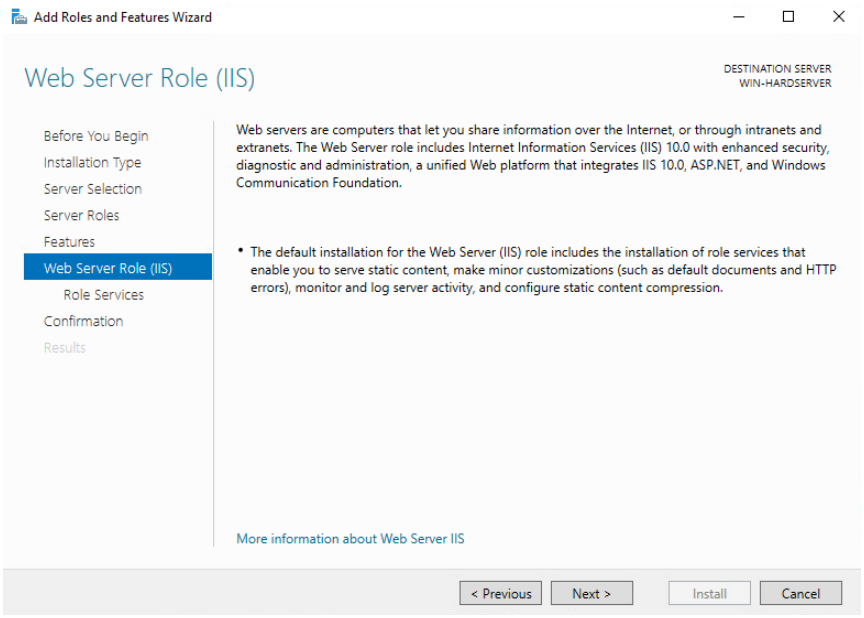
7. When prompted to install Remote Server Administration Tools, select **Add Features** and select **Next**.



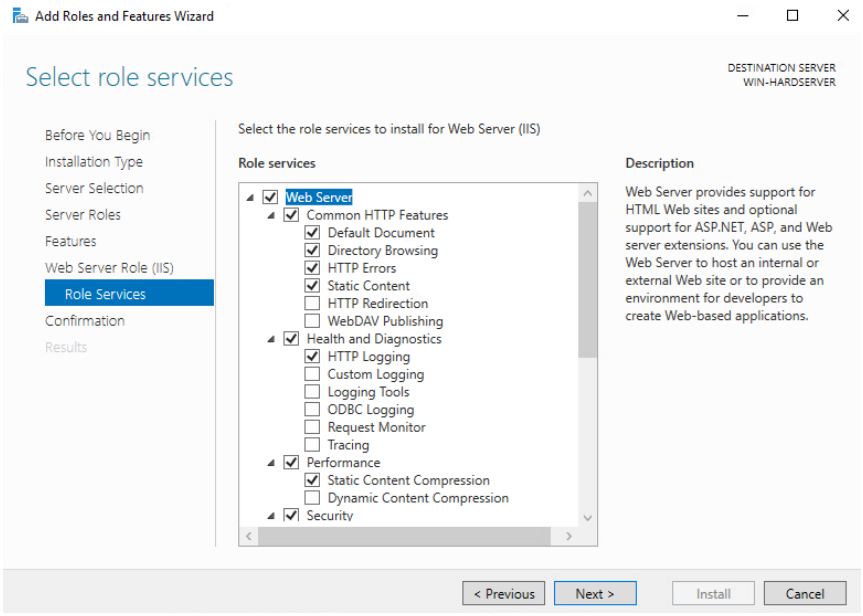
8. On the **Select features** screen, keep the default selection and select **Next**.



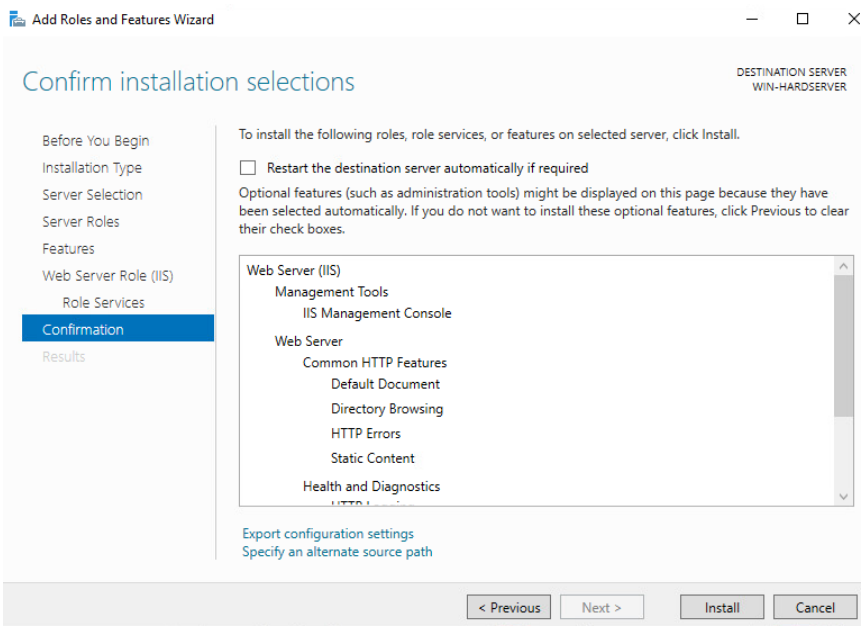
9. On the **Web Server Role (IIS)** screen, select **Next**.



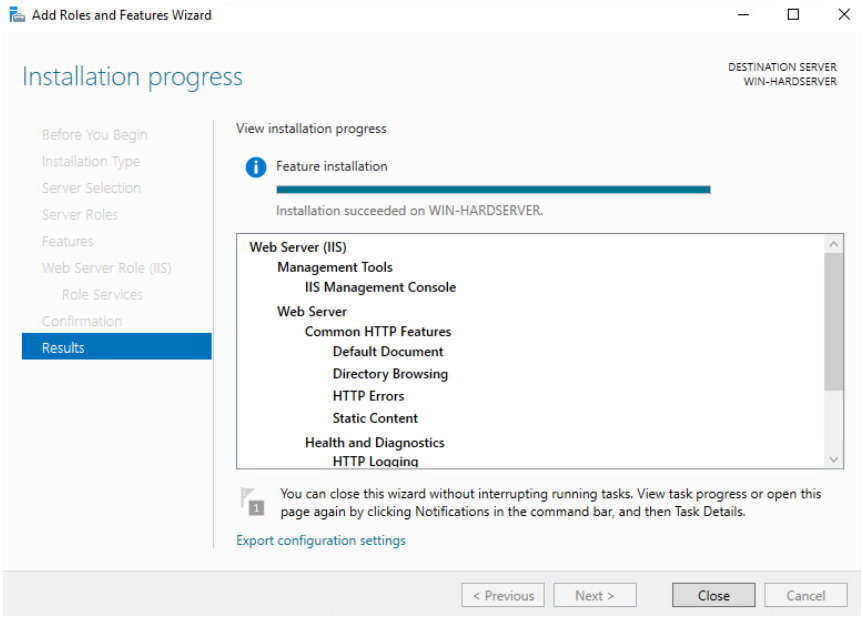
10. On the **Select Role Service** screen, select **Next**.



11. On the confirmation screen, select **Install**.



12. Once the installation completes, Select **Close**.



2.7. Create a certificate request

IIS Manager does not support the creation of certificates protected by CNG Keys and these must be created using the Microsoft command line utilities. Commands executed in this section are run on a PowerShell in Windows.

Due to limitations of IIS itself, no GUI prompts (even via nShield Service Agent) can be displayed, so any OCS protection must be passphrase-less 1/n quorum. For this reason, use only OCS or module protection.

Complete the following steps to create a certificate request:

1. Make sure the nCipher Primitive Provider and nCipher Security World Key Storage Providers are listed:

```
% 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
```

If the `nCipher Primitive Provider` and `nCipher Security World Key Storage Provider` are not listed, follow the steps in Install

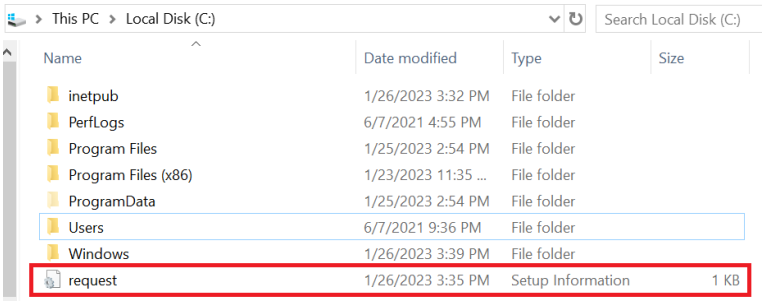
> and register the CNG provider.

2. Set up a template file:
   a. Generate a request for an SSL certificate linked to a 2K RSA key by creating a file called `request.inf` with the following information:

```
[Version]
Signature= "$Windows NT$"
[NewRequest]
Subject = "CN=interop.com,C=US,ST=Florida,L=Sunrise,O=InteropCom,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
```

   Your `request.inf` file can vary from the code given above. This is an example, not a definitive model.

   b. Specify the subject details of the Domain Controller which is issuing the certificate.
   c. Specify the key algorithm and key length as required, for example RSA 2048.
   d. Specify the Provider name as **nCipher Security World Key Storage Provider**.
   e. After you set up the template successfully, save it as `request.inf` on the `C:\` drive.



3. Open a command prompt and go to the local drive, in this case `C:\`.
4. To create the certificate request for the Certification Authority, execute the command:

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

CertReq: Request Created
```

A certificate request called `IISCertRequest.csr` is generated and placed on the `C:\` drive. This file is used to be sent to a Certificate Authority.

2.8. Get the signed certificate

1. Submit the CSR file to a CA such as VeriSign, Entrust, and so on.
2. The CA authenticates the request and returns a signed certificate or a certificate chain.
3. Save the reply from the CA in the current working directory.

In this guide the signed certificate file is `IISCertRequest.cer`.

2.9. Install the certificate

Make the certificate available to be used in IIS and bind the certificate with the https settings in IIS.

Commands used in this section are run from a Windows PowerShell.

2.9.1. Make the certificate available for use in IIS

To make the certificate available for use in IIS, run the following command:

```
% certreq -accept IISCertRequest.cer
```

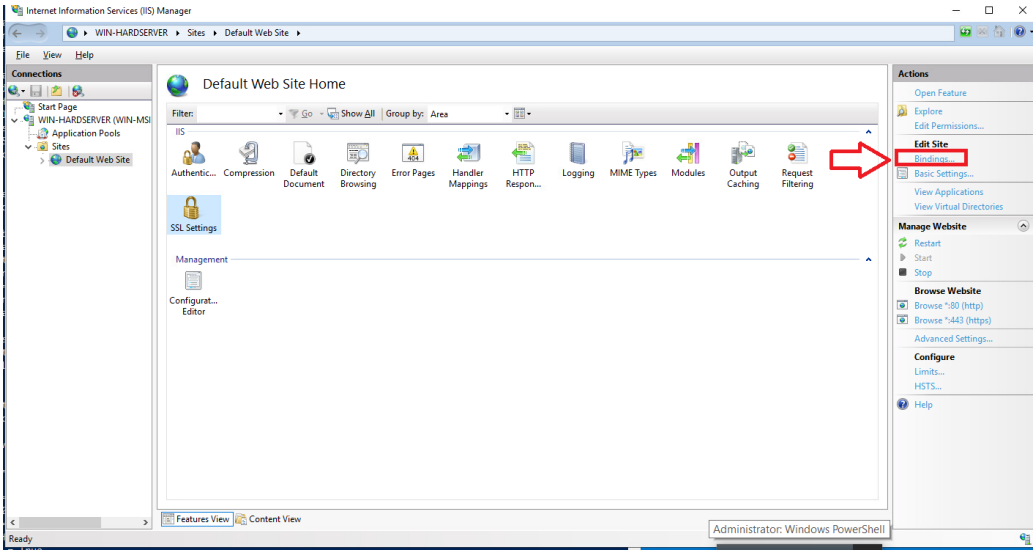
Where `IISCertRequest.cer` is the binary certificate exported from the CA. Running this command makes the CA certificate trusted on the Web Server.

```
Installed Certificate:
  Serial Number: 1c00000002685e0d9d05770729000000000002
  Subject: CN=interop.com, OU=WebServer, O=InteropCom, L=Sunrise, S=Florida, C=US
  NotBefore: 1/25/2023 2:18 PM
  NotAfter: 1/25/2024 2:28 PM
  Thumbprint: 7a814f14f77db1eae717a4c753fd7b184d6a6037
```

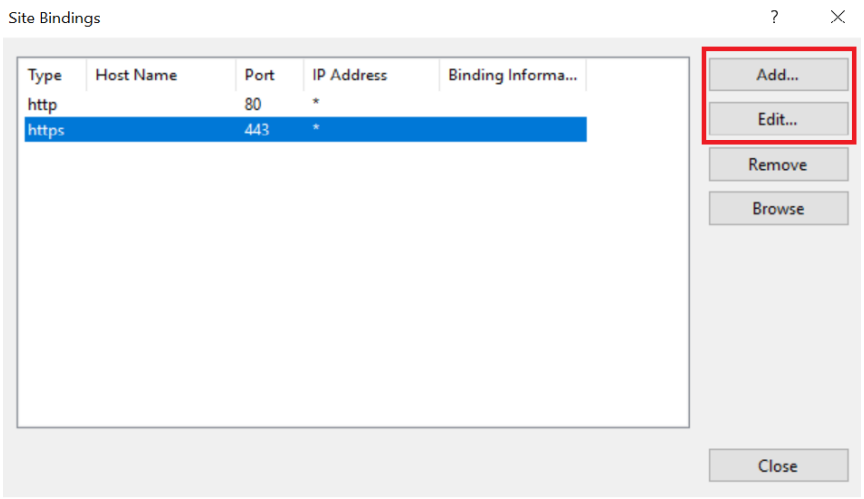
2.9.2. Bind the certificate with a secure IIS web server

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.

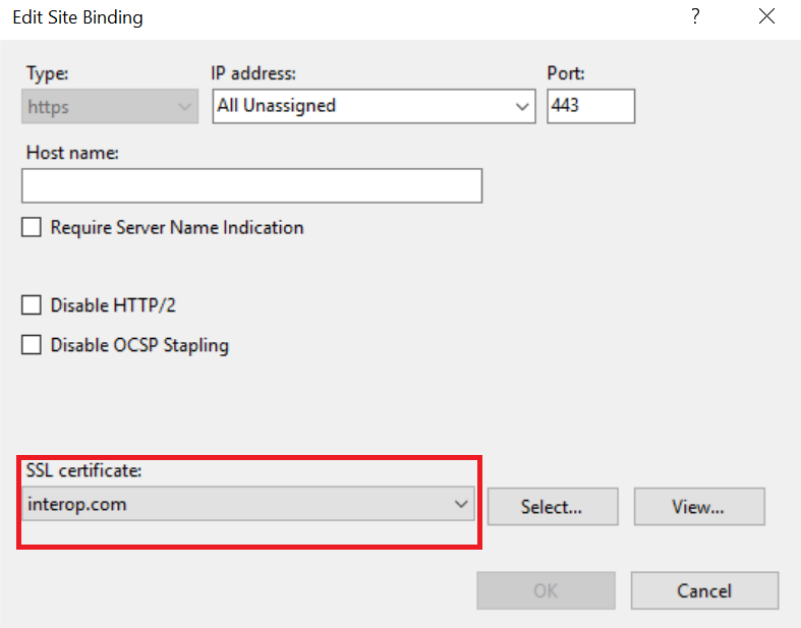
3. Under **Sites** on the left-hand side of the IIS Manager screen, select **Default website**.



4. Select **Bindings** link on the right-hand side of the IIS Manager.
5. Access the **Site Bindings** screen.
6. If the **https** protocol is not listed, you must add it now. To do this, select **Add**, set the protocol as **https** and select the required certificate from the list.



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



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

2.10. Integrate an nShield HSM with an existing IIS deployment

This section describes how to upgrade an existing IIS server installation to use an nShield HSM to protect the private key. It is assumed that the existing certificate must continue to be used by the server afterwards.

The Prerequisites to integrate are:

- An IIS set-up with software-protected certificate and private key.
- nShield Software installed and a Security World created using The CNG Configuration Wizard, or the front panel of an nShield Connect.

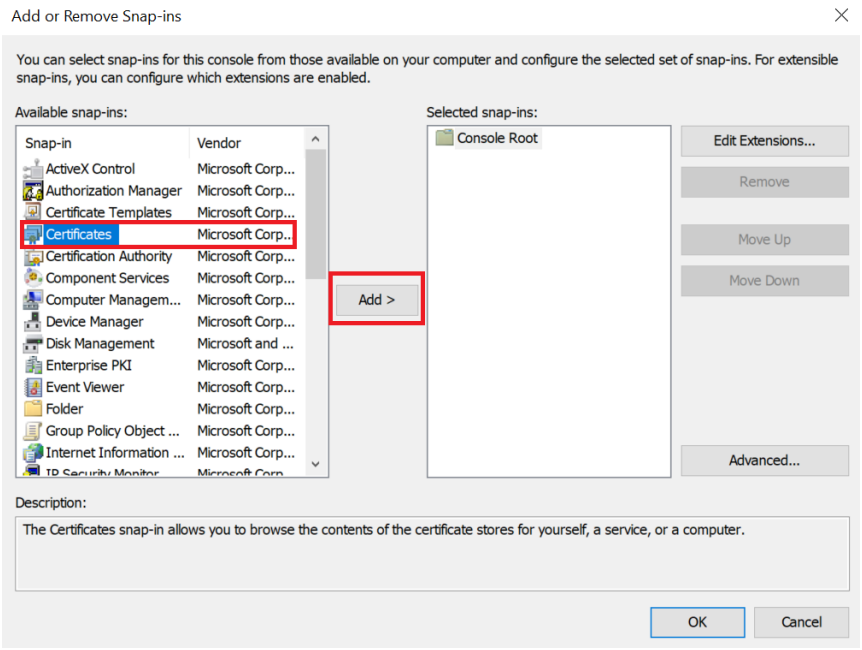
2.10.1. Export the software-protected certificate

Complete the following procedure to export the software-protected certificate:

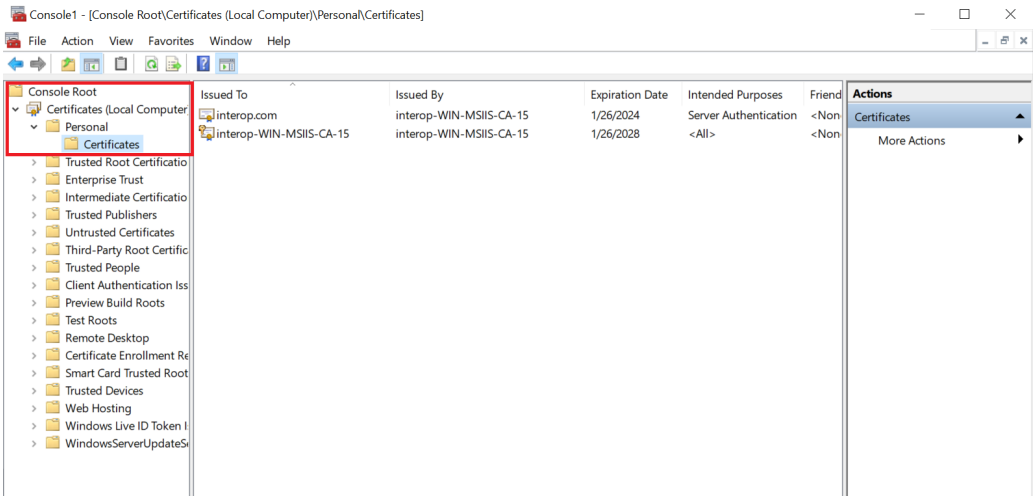
1. Type `MMC` at the command prompt and select **OK**.

   The Microsoft Management Console starts.

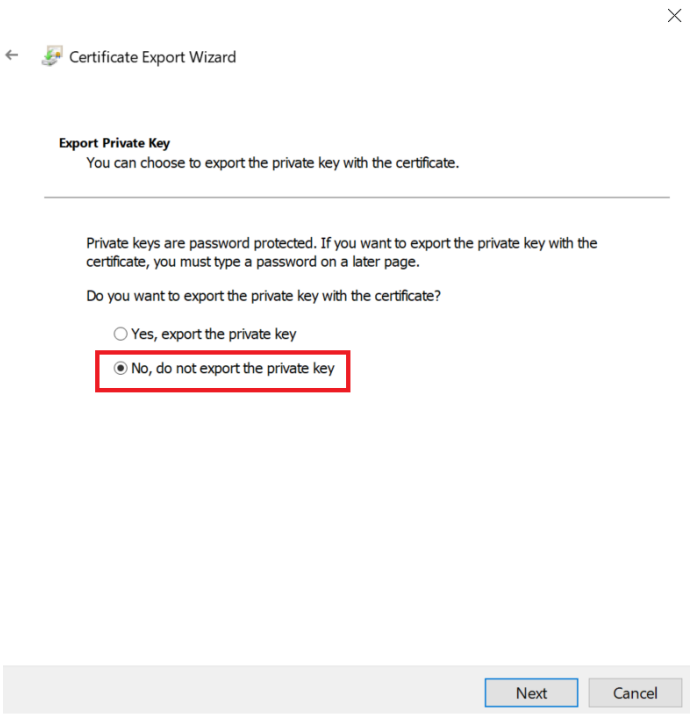
2. On the initial screen, select **File** > **Add/Remove Snap-in** and select **Add**.
3. Select **Certificates** from **Available Standalone Snap-ins** and select **Add**.



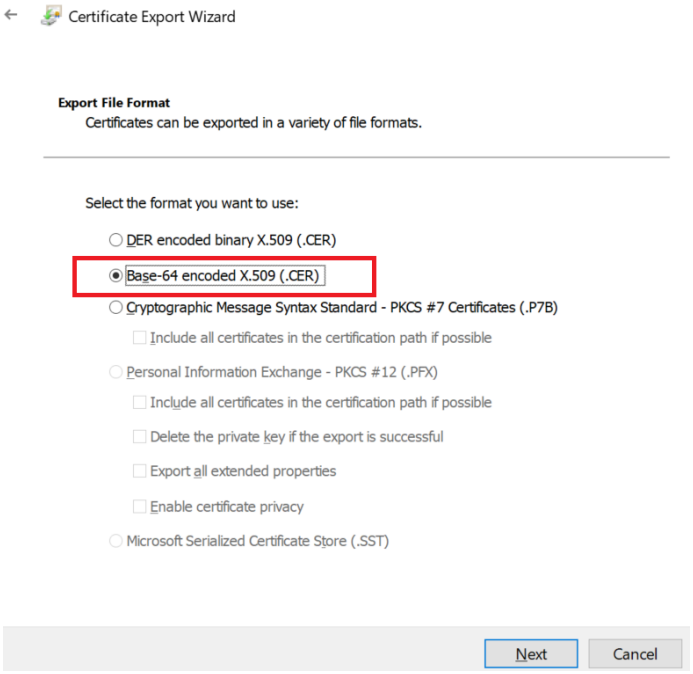
4. On the **Certificates snap-in** screen, select **Computer account** and select **Next**.
5. On the **Select Computer** screen, select **Local computer**, select **Finish** then **OK**.
6. Navigate to **Certificates (Local Computer)** > **Personal** > **Certificates**.



7. Right-select the certificate file and select **All Tasks** > **Export**.
8. The **Welcome to the Certificate Export Wizard** screen appears. Select **Next**.
9. On the **Export Private Key** screen, select **No, do not export the private key** and select **Next**.



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



11. On the **File to Export** screen, select an absolute path and filename to save the exported Certificate.

    Select **Next**.

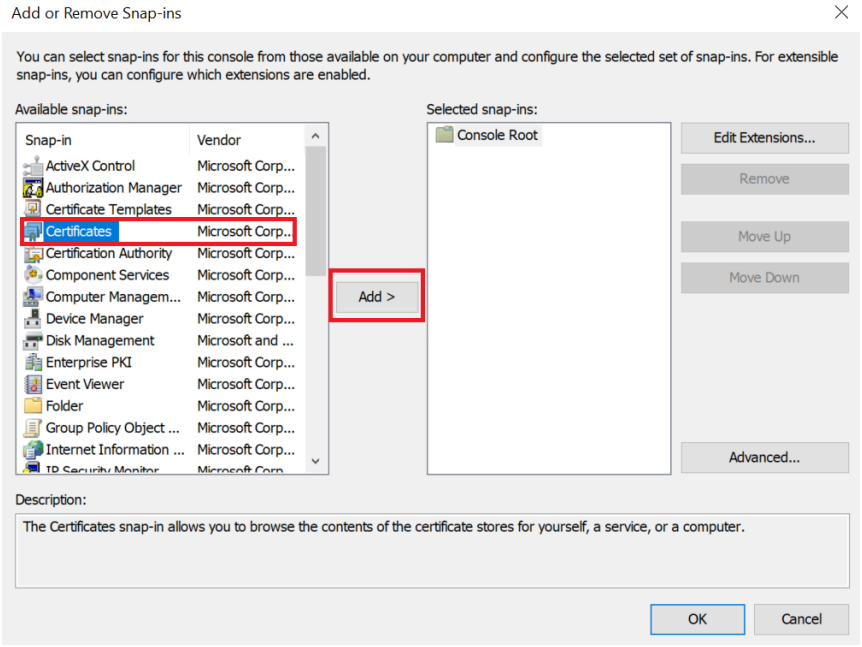
12. The **Completing the Certificate Export Wizard** screen appears.

Select **Finish**.

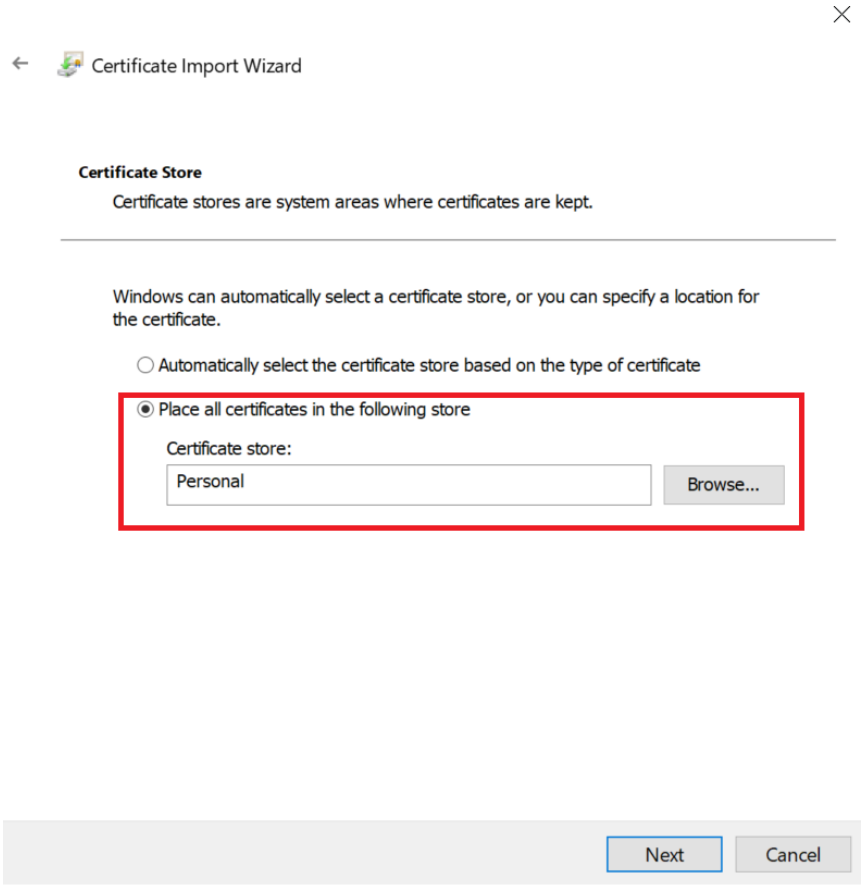
13. After exporting the certificate, delete the certificate from the certificate store.

2.10.2. Import a certificate into the certificate store

1. Go to the command prompt and type `MMC`, then select **OK** to open the Microsoft Management Console.
2. On the initial screen, select **File** > **Add/Remove Snap-in** and select **Add**.
3. From **Available Standalone Snap-ins**, select **Certificates** and select **Add**.



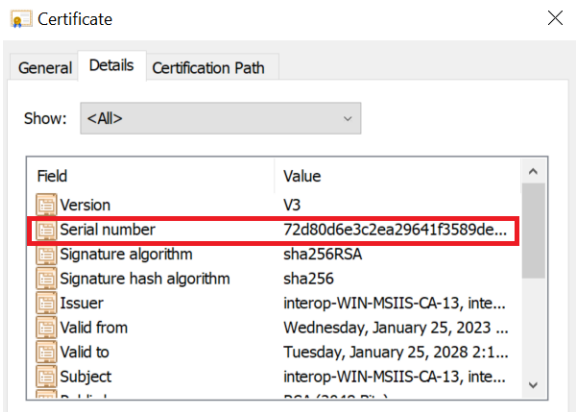
4. On the **Certificates snap-in** screen, select **Computer account** and select **Next**.
5. On the **Select Computer** screen, select **Local computer**, select **Finish** and select **OK**.
6. Navigate to **Certificates (Local Computer)** > **Personal** > **Certificates**.
7. Right-click the certificate folder and select **All Tasks** > **Import**.
8. The **Welcome to the Certificate Import Wizard** screen appears. Select **Next**.
9. Navigate to the location of the certificate from the **Origin Server** and select **Next**.
10. On the **Certificate Store** screen, select **Place all certificates in the following store**.



11. Make sure that the default selection in **Certificate Store** is **Personal**, then select **Next**.
12. The **Completing the Certificate Import Wizard** screen appears.

    Select **Next**, then select **OK**.

13. Locate the serial number for the certificate. To do this on the Microsoft Management Console, access **Certificates**, select the certificate, and select the **Details** tab to see the **Serial Number**.



14. Run the following command from the Windows terminal:

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

15. Open the IIS Manager from **Start** > **Internet Information Services (IIS) Manager**.
16. Under **Sites** on the left-hand side of the **IIS Manager** screen, select the required web site.
17. On the right-hand side of the **IIS Manager** screen, select **Bindings**.
18. On the **Site Bindings** screen, select **Add**.
19. Select the protocol **HTTPS**.
20. Select the certificate from the drop-down list.
21. To complete the certificate binding for SSL connection, select **OK**.

Chapter 3. Appendix

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

To 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
   ```