Microsoft AD CS and NDES

nShield® HSM Integration Guide for Microsoft Windows Server

2023-12-05

Table of Contents

Chapter 1. Introduction

This guide describes how MS NDES can utilize a Microsoft Certificate Authority enrolled with an Entrust nShield Hardware Security Module (HSM) as a Root of Trust for storage encryption, to protect the private keys and meet FIPS 140 Level 2 or Level 3.

The Entrust nShield is also used to protect the NDES Admin web page using TLS, where the private key for the certificate is nShield managed. NDES implements the Simple Certificate Enrollment Protocol (SCEP), which defines the communication between network devices and a Registration Authority (RA) for certificate enrollment.

SCEP supports the secure issuance of certificates to network devices which do not run with domain credentials to enroll for x509 version 3 certificates from a Certification Authority (CA).

Ultimately, the network device will have a private key and associated certificate issued by a CA protected by the Entrust nShield HSM. Applications on the device may use the key and its associated certificate to interact with other entities on the network. The most common usage of this certificate on a network device is to authenticate the device in an IPSec session.

1.1. Product configurations

Entrust tested the integration with the following versions:

Product	Version
Base OS	Windows Server 2019 Datacenter

1.2. Supported nShield hardware and software versions

Entrust tested the integration with the following nShield HSM hardware and software versions:

Product	Security World	Firmware	Netimage
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

1.3. Supported nShield HSM functionality

Feature	Support
Module-only key	Yes
OCS cards	Yes
Softcards	Yes
nSaaS	Yes
FIPS 140 Level 3	Yes

1.4. Requirements

Familiarize yourself with:

- Active Directory Certificate Services (AD CS): Network Device Enrollment Service (NDES) documentation (https://docs.microsoft.com).
- The *Installation Guide* and *User Guide* for the HSM.
- Your organizational Certificate Policy and Certificate Practice Statement and a Security Policy or Procedure in place covering administration of the PKI and HSM:
  - The number and quorum of Administrator cards in the Administrator Card Set (ACS) and the policy for managing these cards.
  - The number and quorum of operator cards in the Operator Card Set (OCS) and the policy for managing these cards.
  - The keys protection method: Module, Softcard, or OCS.
  - The level of compliance for the Security World, FIPS 140 Level 3.

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

◦ Key attributes such as key size, time-out, or need for auditing key usage.

Chapter 2. Procedures

Prerequisites:

- A Windows domain controller.
- Domain administrator privileges to add accounts and join clients.
- A Windows server in the domain with Internet Information Services (IIS) installed Active Directory Certificate Service (AD CS) will be installed in this server per the instructions below.
- A second Windows server in the domain with IIS installed. NDES will be installed in this server per the instructions below.
- A Windows client in the domain to request CA hash and challenge password pairs.

Installation steps:

1. Select the protection method
2. Install the Security World software and create a Security World
3. Generate the OCS or Softcard in the CA server
4. Configure the CNG provider in the CA server
5. Configure the CNG provider on the NDES server
6. Install and configure AD CS on the CA server
7. Add certificates templates to the CA server
8. Create a virtual directory to serve as the public key infrastructure (PKI) repository
9. Create domain user accounts to act as the NDES service account
10. Add the SCEPAdmin account and SCEPSvc service account to the local IIS_IUSRS group
11. Configure the SCEPAdmin account and SCEPSvc service account with request permission on the CA
12. Configure the SCEPDeviceAdmin account with enroll permission to the IPsec (offline request) certificate template
13. Install and configure NDES
14. Configure the NDES admin page to use an SSL certificate

2.1. Select the protection method

OCS, Softcard, or Module protection can be used to authorize access to the keys

protected by the HSM. Follow your organization's security policy to select which one. The following protection methods were used in this integration:

- HSM OCS with passphrase protection was used to protect the CA. This is the highest level of protection.
- HSM Module protection was used to generate the certificate request for IIS binding for secure access to the NDES server. IIS binding is only possible with:
  - OCS without a passphrase
  - Module protection
- Microsoft cryptography provider was used to protect the RA keys. For RA keys, only Cryptographic Application Programming Interface (CryptoAPI) Service Providers are supported.

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

1. Log into the CA server using the domain name, <domain_name>\Administrator.
2. Install the Security World software by double-clicking on the `SecWorld_Windows-xx.xx.xx.iso` file. For detailed instructions, see the *Installation Guide* and the *User Guide* for the HSM.
3. Add the Security World utilities path `C:\Program Files\nCipher\nfast\bin` to the Windows system path.
4. Open the firewall port 9004 outbound for the HSM connections.
5. 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.

6. Open a command window and run the following to confirm the HSM is `operational`:

```
C:\Users\dbuser>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.
 ...
```

7. Create your Security World if one does not already exist, or copy an existing one. Follow your organization's security policy for this. ACS cards cannot be duplicated after the Security World is created. Create a quorum K/N appropriate for your implementation and to protect against card failure or loss.

8. Confirm the Security World is `usable`:

```
C:\Users\dbuser>nfkminfo
World
 generation  2
 state       0x37270008 Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
```

9. Log into the NDES server using the domain name, <domain_name>\Administrator and repeat the above steps, but copying the Security World from the CA server.

2.3. Generate the OCS or Softcard in the CA server

To create the OCS:

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 created. Enter a passphrase or password at the prompt. Notice `slot 2`, remote via a Trusted Verification Device (TVD), is used to present the card. In this example, K=1 and

N=1.

```
>createocs -m1 -s2 -N MSaDCSnDESocs -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 card
 Module 1 slot 2:- passphrase specified - writing card
Card writing complete.

cardset created; hkltu = 8b652e480d6307c32a1b1395a7a12c8ef07fbd24
```

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 need to 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
 8b652e480d6307c32a1b1395a7a12c8ef07fbd24  1/1  none-NL MSaDCSnDESocs
```

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

If you are using Softcard protection, create the Softcard now.

1. Ensure the `C:\Program Files\nCipher\nfast\cknfastrc` file exists with the following content. Otherwise create it.

```
> type "C:\Program Files\nCipher\nfast\cknfastrc"
CKNFAST_LOADSHARING=1
```

2. Execute the following command and enter a passphrase/password at the prompt:

```
>ppmk -n MSaDCSnDESsoftcard

Enter new pass phrase:
Enter new pass phrase again:
New softcard created: HKLTU f2f7d34e4ddc950038db430ddbe06488f4c21ee7
```

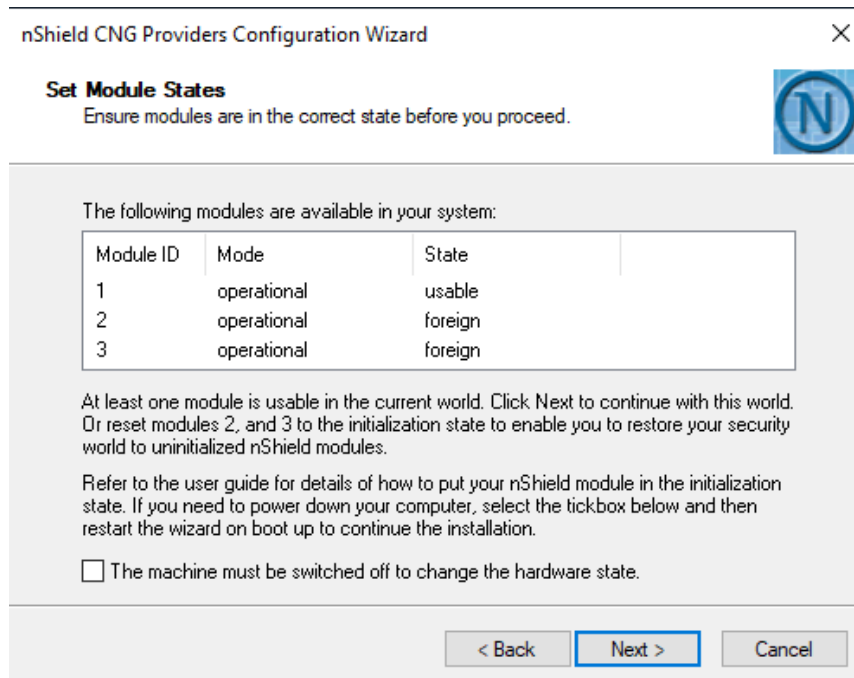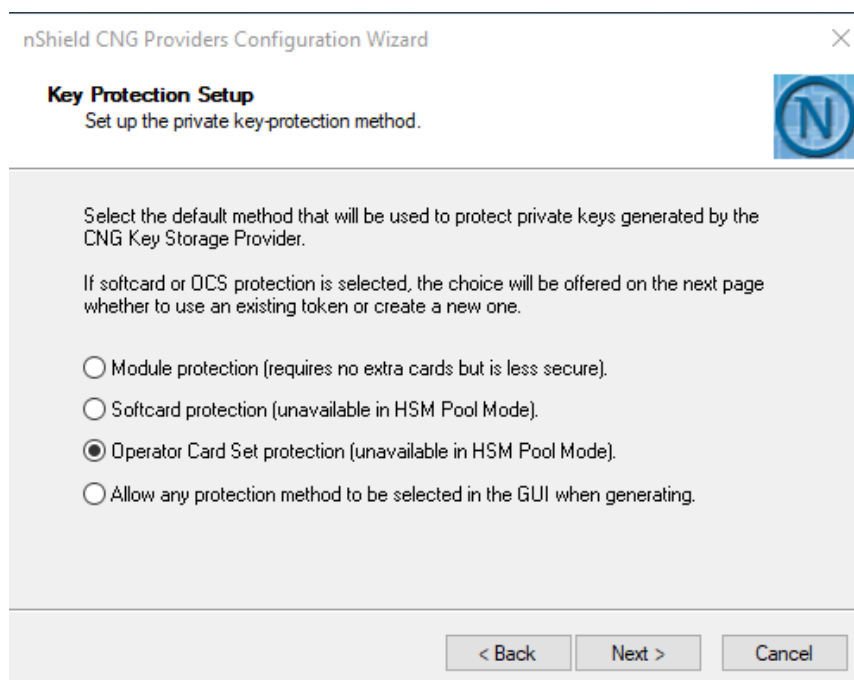3. Verify the Softcard was created:

```
>nfkminfo -s
SoftCard summary - 1 softcards:
 Operator logical token hash               name
 f2f7d34e4ddc950038db430ddbe06488f4c21ee7  MSaDCSnDESsoftcard
```

The `rocs` utility also shows the OCS and Softcard created.

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

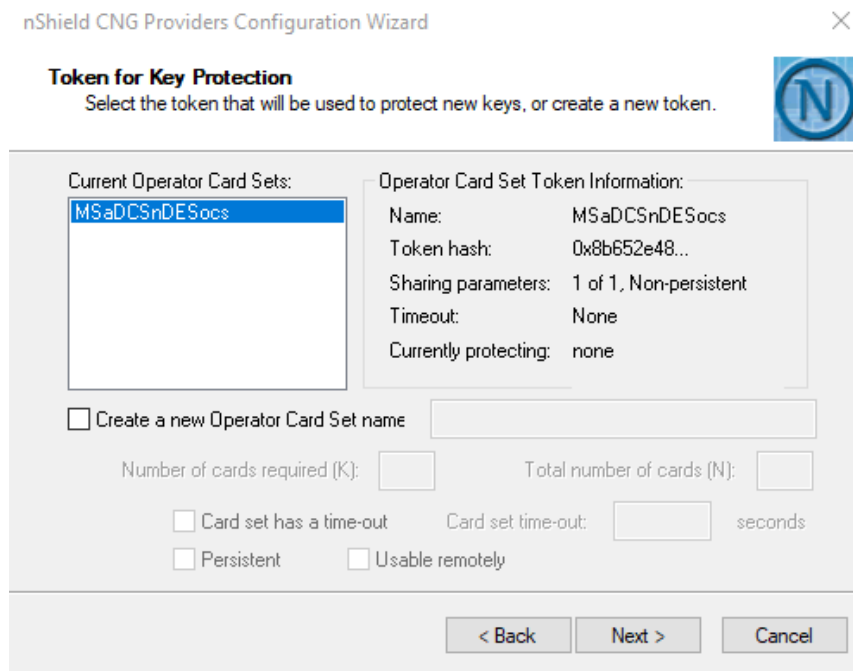# 2.4. Configure the CNG provider in the CA server

1. Log into the CA server using the domain name, <domain_name>\Administrator.

2. Select **Start** > **nCipher** > **CNG configuration wizard**.

3. Select **Next** on the **Welcome** window.

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

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

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

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

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

9. Verify the provider with the following command:

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

2.5. Configure the CNG provider on the NDES server

1. Log into the NDES server using the domain name,
   <domain_name>\Administrator.

2. Select **Start > nCipher > CNG configuration wizard**, then follow the steps to
   configure the CNG as described in Configure the CNG provider in the CA
   server.

2.6. Install and configure AD CS on the CA server

1. Log into the CA server using the domain name,
   <domain_name>\Administrator.

2. Select **Start > Server Manager** to open the Server Manager.

3. Select **Manage**, then select **Add Roles & Features**. The **Before you begin**
   window appears. Select **Next**.

4. Select **Role-based or feature-based installation** on the **Select installation
   type** window. Select **Next**.

5. Select the local server from the pool on the **Select destination server** window. Select **Next**.

6. Select **Active Directory Certificate Services** role on the **Select server roles** window. The **Add Roles and Features** Wizard will appear. Select **Add Features** and then select **Next**.

7. In **Select features**, select **Next**.

8. Select **Next** on the **Active Directory Certificate Services** window.

9. Select **Certification Authority** on the **Select role services** windows.

10. Select **Next**.

11. Verify the information, then select **Install** on the **Confirm installation selections** window.
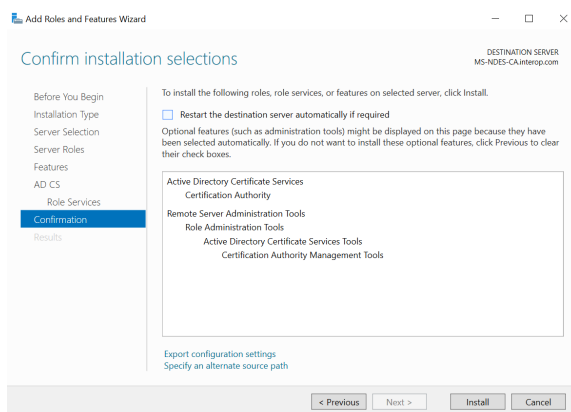
12. Do not select **Close** the **Installation progress** windows once the installation is complete. Instead, select the **Configure Active Directory Certificate Services on the destination server** link.
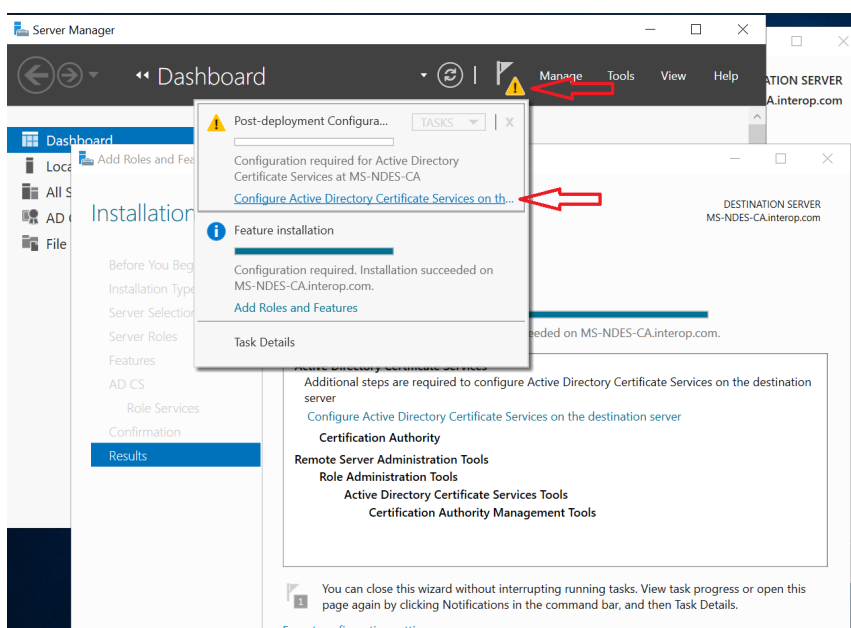
13. Verify the **Administrator** credentials, <domain_name>\Administrator on the **Credentials** text box on the **Credentials** windows. If needed select **Change** and specify the appropriate credentials. Select **Next**.

14. Select **Certification Authority** on the **Role Services** window. This is the only available selection when the certification authority role is installed on the server. If using OCS key protection, present the OCS card in the HSM or TVD. When the communication with the HSM has been established the button becomes active. Select **Next**.

15. Select **Enterprise CA** on the **Setup Type** window. Select **Next**.

16. Select **Root CA** on the **CA Type** window. Select **Next**.

17. Select **Create a new private key** on the **Private Key** window. Select **Next**.

18. In **Cryptography for CA > nCipher Security World Key Storage Provider**, select a provider with key length 2048 or longer. Also check **Allow administrator interaction when the private key is accessed by the CA** if OCS or Softcard protection is used, our case in this integration. Then select **Next**.

19. Take the default CA name given, or modify if required on the **CA Name** window. Select **Next**.

20. Enter the number of years for the certificate to be valid on the **Validity Period** window. Select **Next**.

21. Take the default locations for the database and database log files, or modify if required on the **CA Database** window. Select **Next**.

22. Select **Configure** on the **Confirmation** window.

23. A **Create new key** wizard window appears on the task bar. It may be hidden behind the other windows. Open it and select **Next**.

24. Select the protection method for the new key, **Operator Card Set protection** for this integration. Select **Next**.

> **ℹ** You will be prompted to enter the Softcard passphrase or present the OCS (token) if either protection method was chosen when the CNG provider was installed. There will be no prompt if Module protection was chosen.

> **ℹ** If you are using a FIPS 140 Level 3 Security World, you will need to present either a card from the ACS or OCS for FIPS authorization before the AD CS key can be generated, irrespective of your chosen protection method.

25. Present the Softcard passphrase or OCS and select the module if more than one nShield Connect is available. Select **Finish** to close the wizard. The

following image shows when OCS protection is selected.
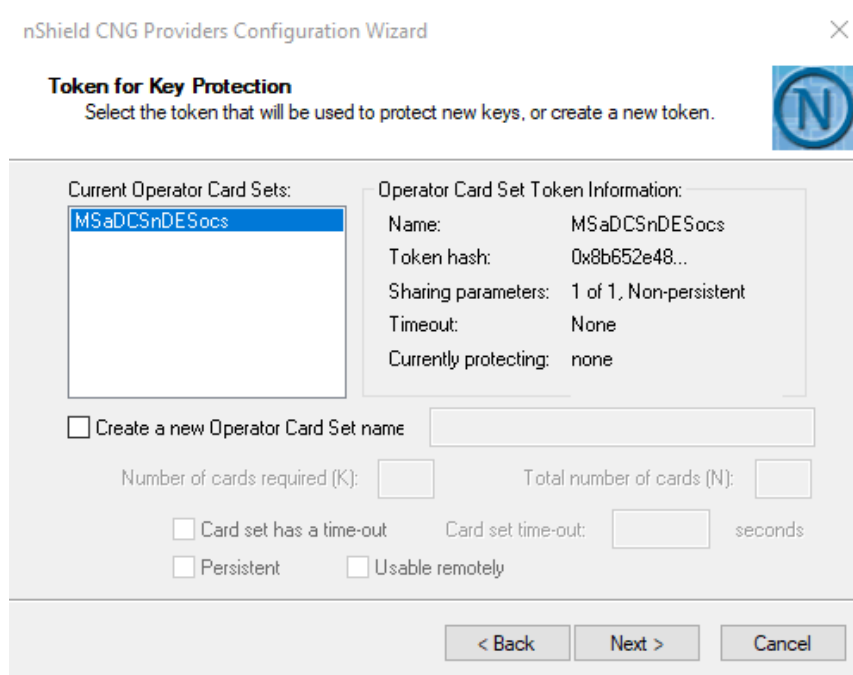
26. Select **Next** on the **Load key** window.

27. Select the module on the **Choose modules you wish to load the key onto** window. Select **Next**.

28. Enter the passphrase. Select **Next**. You may be prompted more than once for the same information.

29. Select **Finish**. Successful configuration is shown as follows. Select **Close**.
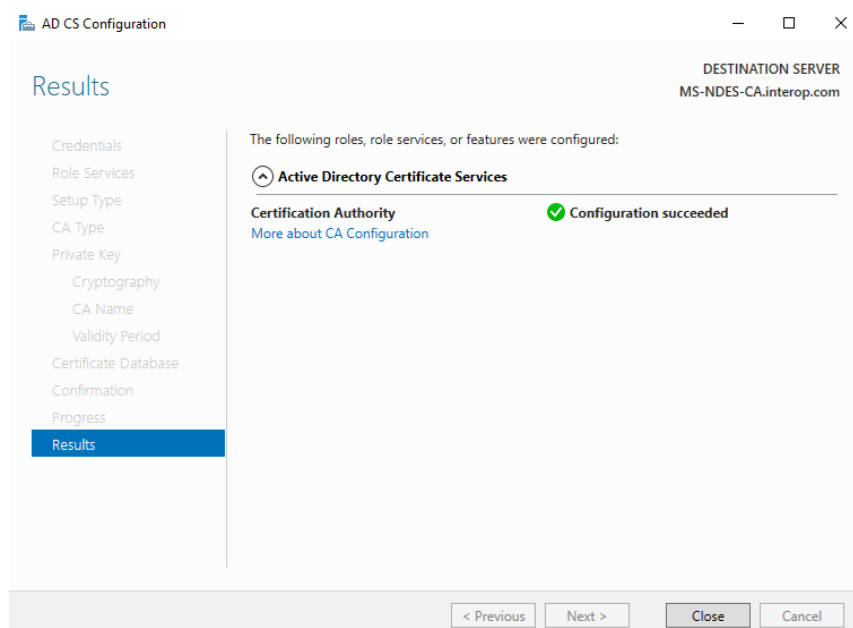
30. The key generated can be verified using a CLI command:

```
>nfkminfo -l

Keys protected by cardsets:
 key_caping_machine--75393afa6878b98e3d91b5ff360284f706a97572 `interop-MS-NDES-CA-CA`
```

The `rocs` utility shows the names and protection methods of the keys.

```
>rocs
`rocs` key recovery tool
Useful commands: `help`, `help intro`, `quit`.
rocs> list keys
  No. Name                    App       Protected by
    1 interop-MS-NDES-CA-CA    caping    MSaDCSnDESocs
rocs> quit
```

31. Register `nFast Server` as a dependency of AD CS with the `ncsvcdep` tool in the `nfast/bin` directory. This is needed as the nShield service must have started before CA, otherwise the nShield CNG providers will fail.

    Run the command:

    ```
    >ncsvcdep -a certsvc
    ```

    Example output:

    ```
    Dependency change succeeded.
    ```

32. Verify that the CA service has started successfully.

    Run the command:

    ```
    >sc query certsvc
    ```

    Example output:

    ```
    SERVICE_NAME: certsvc
            TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
            STATE              : 4  RUNNING
                                    (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
            WIN32_EXIT_CODE    : 0  (0x0)
            SERVICE_EXIT_CODE  : 0  (0x0)
            CHECKPOINT         : 0x0
            WAIT_HINT          : 0x0
    ```
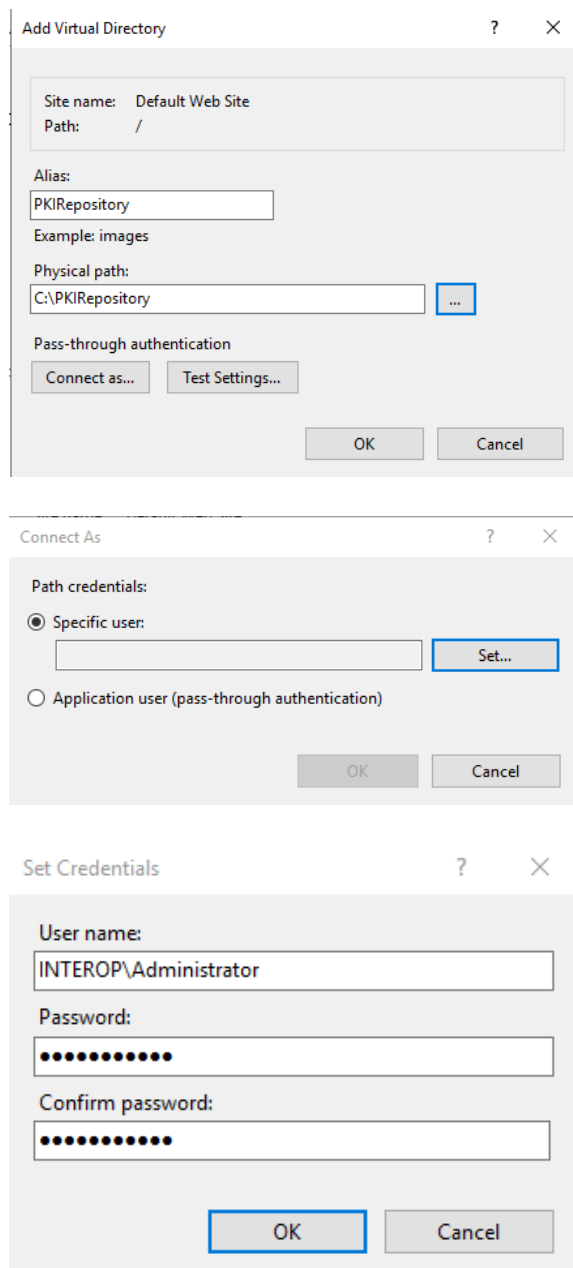
33. In **Installation progress**, select **Close**.

2.7. Add certificates templates to the CA server

1. Sign in to the CA server using *<domain_name>\Administrator*.

2. Select **Server Manager > Tools > Certification Authority**.

3. Expand the issuing CA node in the left-hand pane.

4. Right-click **Certificate Templates**, then select **New > Certificate Template to Issue**.

5. Select the following templates, then select **OK**:

   - **EnrollmentAgentOffline**

   - **CEPEncrytion**

   - **IPSEC (Offline request)**

6. Check that the templates have been added.
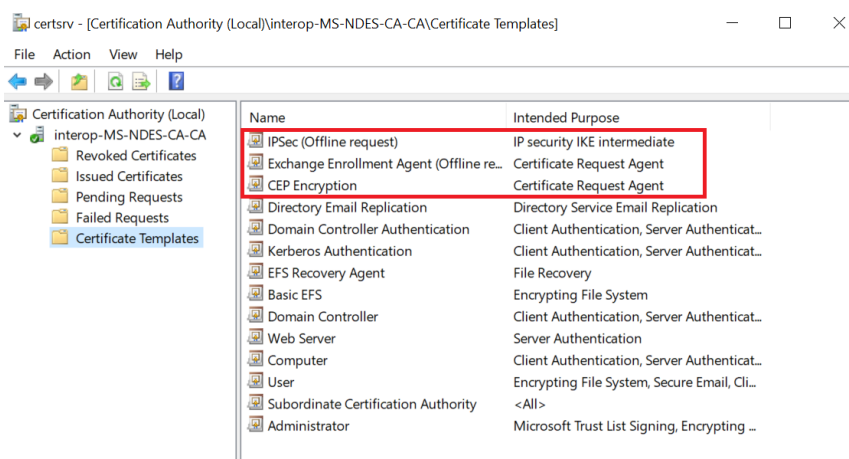
2.8. Create a virtual directory to serve as the public key infrastructure (PKI) repository

1. Log into the CA server using the domain name, <domain_name>\Administrator.

2. Create a local directory for PKI repository, for example `C:\PKIRepository`. See the following Microsoft link for instructions, https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/create-virtual-directory-folder-remote-computer.

3. Create a virtual directory. Notice the alias, physical path, and path credentials.

4. Test the virtual directory per the same link above.

2.9. Create domain user accounts to act as the NDES service account

1. Log into the Domain Controller as Domain Administrator.
2. Select **Active Directory Users and Computers** from the **Start** menu.

Add users **SCEPAdmin**, **SCEPSvc**, and **SCEPDeviceAdmin**.

1. Expand <domain_name>.com, right-click on **Users** and select **New** > **User**.

2. Enter the name **SCEPAdmin** and select **Next**. Follow your organization's security policies to set the password. Never expires was selected for the purpose of this integration.

3. Create new users for **SCEPSvc** and **SCEPDeviceAdmin** by repeating the previous steps.

Add user **SCEPAdmin** to the **Enterprise Admins** and **Domain Admins** groups.

1. Right-click on **Enterprise Admins** on the right pane and select **Properties**.
2. Select the **Members** tab and then select **Add**.
3. Enter the **SCEPAdmin** account, select **Check Names**, and if found then select **OK**.
4. Select **Apply** and **OK**.
5. Repeat the above steps for the **Domain Admins** group.

2.10. Add the SCEPAdmin account and SCEPSvc service account to the local IIS_IUSRS group

1. Log into the NDES server using the domain name, <domain_name>\Administrator.
2. Open **Computer Management** (`compmgmt.msc`).

3. Expand **Local User and Groups** on the **Computer Management** console tree, under **System Tools**. Select **Groups**.

4. Double-click **IIS_IUSRS** on the details pane.

5. Select **Add** on the **IIS_IUSRS Properties** window.

6. Enter the **SCEPAdmin** account, select **Check Names**, and if found then select **OK**.

7. Select **Apply** and **OK**.
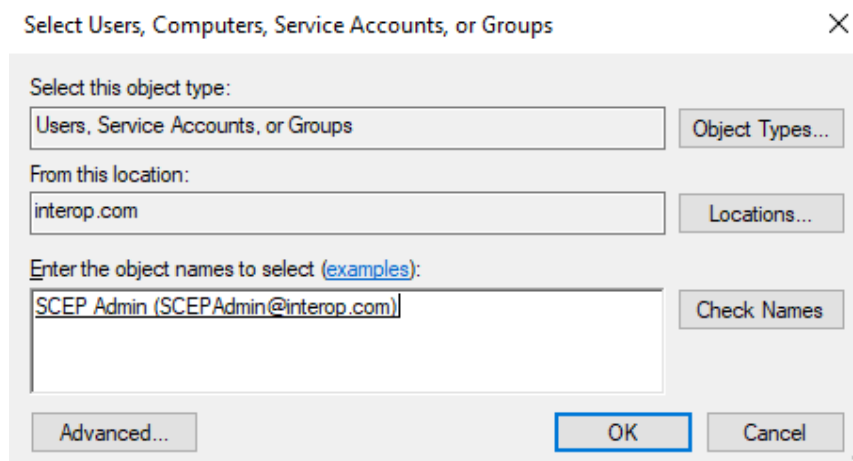
8. Repeat the above steps for the SCEPSvc service account.

2.11. Configure the SCEPAdmin account and SCEPSvc service account with request permission on the CA

1. Log into the CA server using the domain name, <domain_name>\Administrator.

2. Select **Certification Authority** from the **Tools** menu on the **Server Manager** window.

3. Right-click the certification authority (this CA server) and then select **Properties**.

4. Select the **Security** tab.

> Notice the accounts that have **Request Certificates** permissions. By default the group **Authenticated Users** has this permission. The **SCEPAdmin** account will be a member of **Authenticated Users** when it is in use, which has **Request Certificates** permission. However, if that is not the case, do as follows:

5. Select **Add**.

6. On the **Select Users, Computers, Service Accounts, or Groups** text box, type the name of the **SCEPSrv** account, select **Check Names**, and if found select **OK**.

7. Select the **SCEPSrv** account and select the **Allow** check box that corresponds to **Request Certificates**.

8. Select **Apply** and then select **OK**.
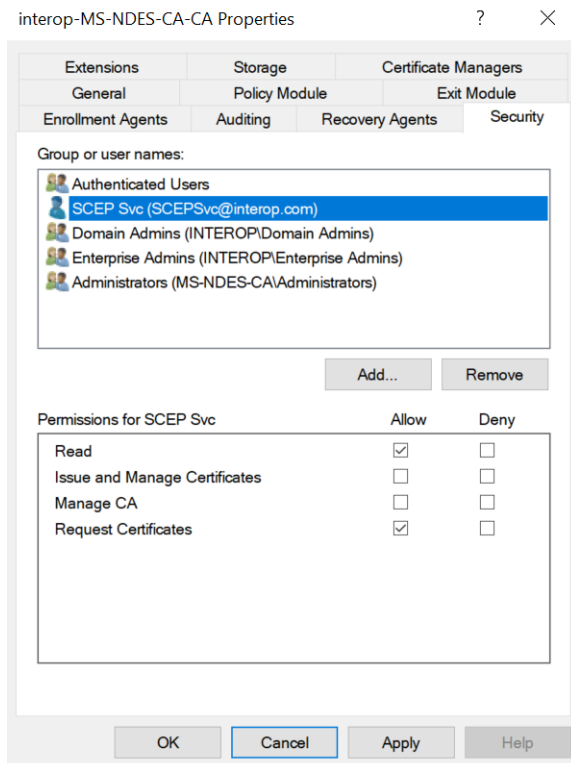
2.12. Configure the SCEPDeviceAdmin account with enroll permission to the IPsec (offline request) certificate template

1. Log into the CA server using the domain name, <domain_name>\Administrator.

2. Select **Certification Authority** from the **Tools** menu on the **Server Manager** window.

3. Expand the server on the left pane, then right-click on **Certificate Templates** and select **Manage**.

4. Right-click **IPSec** on the **Template Display Name** pane and select **Properties**.

5. Select the **Security** tab. Then select **Add**.

6. On the **Select Users, Computers, Service Accounts, or Groups** text box, type the name of the **SCEPDeviceAdmin** account, select **Check Names**, and if found then select **OK**.

7. Select the **SCEPDeviceAdmin** account and verify the **Allow** check box that corresponds to **Enroll** is selected. Select **Apply** and then select **OK**.

2.13. Install and configure NDES

1. Log into the NDES server using the domain name, <domain_name>\Administrator.

2. Select **Start > Server Manager** to open the Server Manager.

3. Select **Manage**, then select **Add Roles & Features**. The **Before you begin** window appears. Select **Next**.

4. Select **Role-based or feature-based installation** on the **Select installation type** window. Select **Next**.

5. Select the local server from the pool on the **Select destination server** window. Select **Next**.

6. Select **Active Directory Certificate Services** role on the **Select server roles** window. The **Add Roles and Features** Wizard appears. Select **Add Features** and then select **Next**.

7. Select **Next** on the **Select features** window.

8. Select **Next** on the **Active Directory Certificate Services** window.

9. Uncheck **Certification Authority** and check **Network Device Enrollment Service** on the **Select role services** window. The **Add Roles and Features** Wizard will appear.

10. Select **Add Features** and then select **Next** on the **Select role services** window.

11. Verify the information, then select **Install** on the **Confirm installation selections** window.

12. Do not select **Close** on the **Installation progress** windows once the installation is complete. Select the **Configure Active Directory Certificate Services on the destination server** link instead.

13. Change the **Credentials** to <domain_name>\SCEPAdmin on the **Credentials** windows. Select **Change**, enter new credential, then select **Next**.

14. From **Select Role Services to configure**, select **Network Device Enrollment Service**, then select **Next**.

15. Select the **Specify service account** on the **Service Account** window, then select **Select…**.

16. Enter the credential for the **SCEPSvc** service account and then select **OK** and **Next**.

17. Select **CA name** on the **CA for NDES** windows, then select **Select...**.

18. Choose the CA server on the **Select Certificate Authority** window, then select **OK** and **Next**.

19. Note the specified Registration Authority (**RA Name**) on the **RA Information** window. Complete any of the optional information as required. Then select **Next**.

20. Choose the **Signature key provider** and **Encryption key provider** on the **Cryptography for NDES** window. A key size of 2048 or larger is recommended.
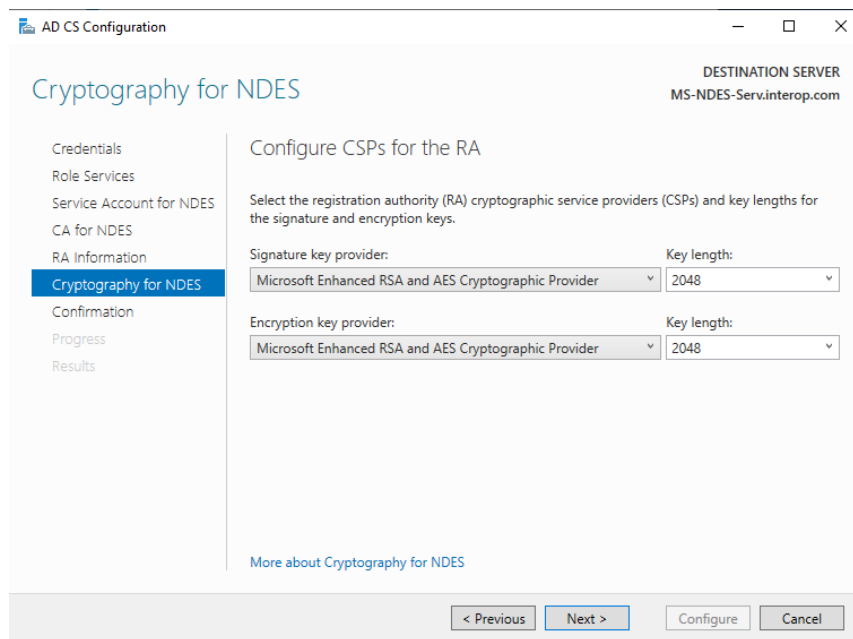
21. Select **Next** and review the chosen options at the **Confirmation** window. Then select **Configure**.

22. Log into the CA server and present the OCS or enter the passphrase if either OCS or Softcard protection was selected. Look for an icon on the **Taskbar** if the **Load key** window is not present. You may be prompted to present the OCS or enter the passphrase more than once.

23. Go back to the NDES server. Notice the **Configuration succeeded** message on the **Results** window. Then select **Close**.

Test access to the NDES web site (unsecured).

> In this example, the **SCEPSrv** account was used for testing access to the NDES web site. Consult your security team and reference Microsoft best practices for deploying in a production environment.

1. Log into the Windows client.

2. Launch the browser and go to the following address: http://<NDES-server-address>/CertSrv/mscep_admin. Log in as <domain-name>\SCEPSvc.
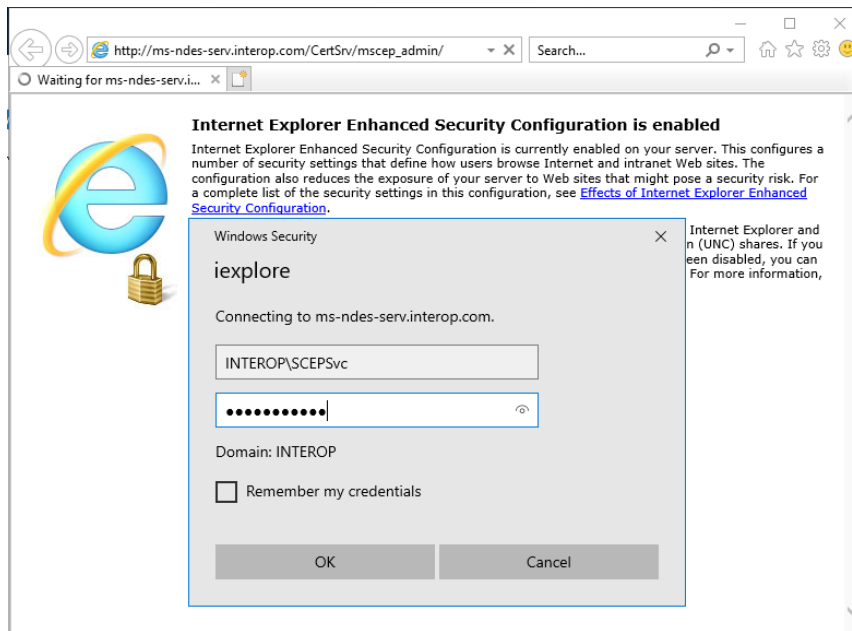
3. Notice the hash value of the CA certificate and the challenge password. Refreshing the browser generates a new challenge password.
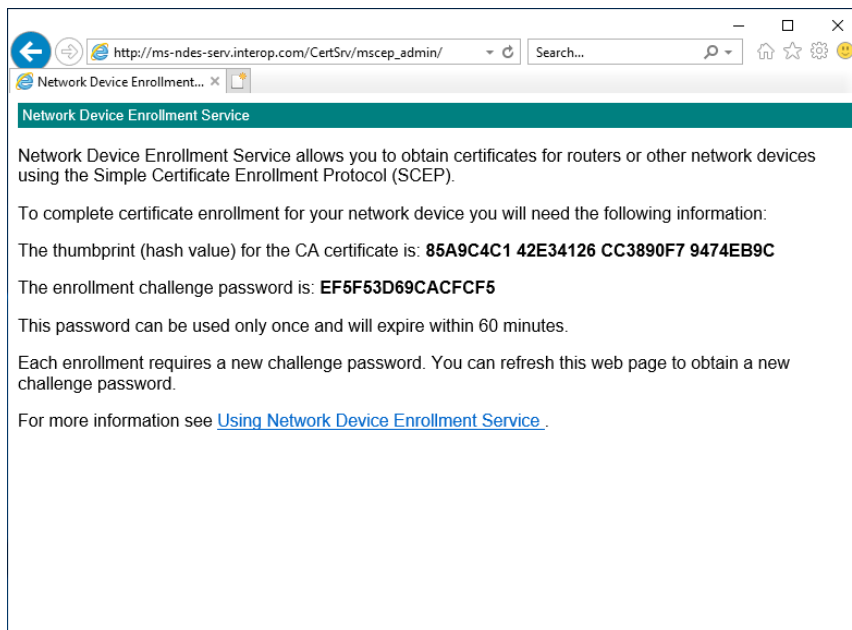
 An unsecure HTTP address to access NDES server is only done above to demonstrate NDES is running. You may want to configure your HTTP address to be redirected to HTTPS for the devices requesting to be enrolled. Refer to Microsoft documentation to perform this configuration.

2.14. Configure the NDES admin page to use an SSL certificate

Create a template for the NDES Admin web service certificate request to ensure that the nCipher KSP is used to generate the key pair.

1. Log into the NDES server using the domain name, <domain_name>\Administrator.

2. Create a `request.inf` file using a text editor as follows. Change **Subject** to the Fully Qualified Domain Name (FQDN) of the NDES Server, for example: `ms-ndes-serv.interop.com`.

```
[Version]
Signature= "$Windows NT$"
[NewRequest]
Subject = "CN=<FQDN-of-NDES-Server>"
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
```

For example:

```
[Version]
Signature= "$Windows NT$"
[NewRequest]
Subject = "CN=ms-ndes-serv.interop.com"
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. Create a Certificate request file by running the following command. Select **Module protection** when prompted.
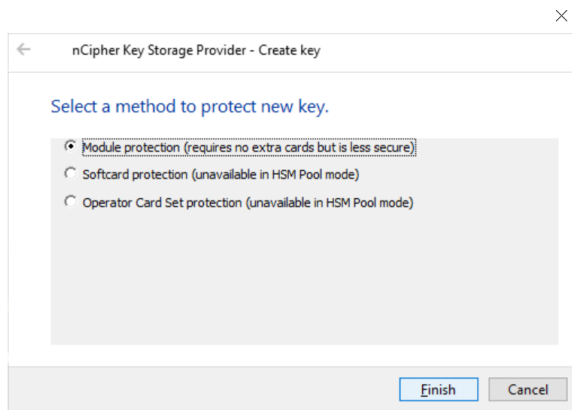
```
certreq.exe -new <Path-to-Request.inf> <Name-of-Request>.req
```

Example output:

```
>certreq -new NDES-SSL-Cert.inf NDES-SSL-Cert.req

CertReq: Request Created
```

4. Copy the above certificate request file to the CA server.

Have the CA issue a certificate based on the Web service certificate template and the certificate request above.

 In this example, **Authenticated Users** is used for provisioning certificates. Consult your security team and reference Microsoft best practices for deploying in a production environment.

1. Log into the CA server using the domain name, **<domain_name>\Administrator**.

2. Enable the **Web Server** certificate template option. Open the **Certification Authority** tool and expand the issuing CA node on the left hand pane.

3. Right-click on **Certificate Templates** and select **Manage**.

4. Right-click on **Web Server** and select **Duplicate Template** on the **Certificate Template Console** window.

5. Select the **General** tab in the **Properties of New Template** dialog. Type the name you want to use on the **Template Display Name**. Then select **Apply** and **OK**.
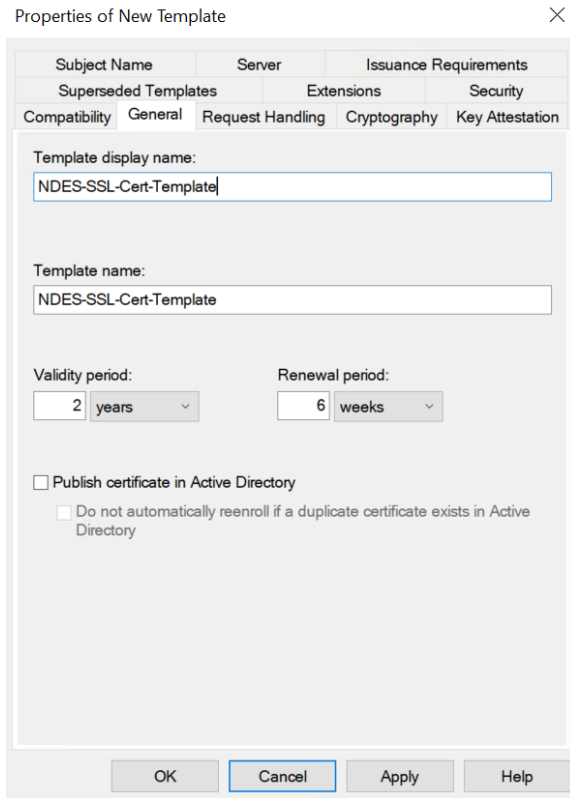
6. Select the **Security** tab.

7. Select **Authenticated Users** in **Groups and user names**. Then check **Enroll** in
   Permissions for Authenticated Users. Then select **Apply** and **OK**.
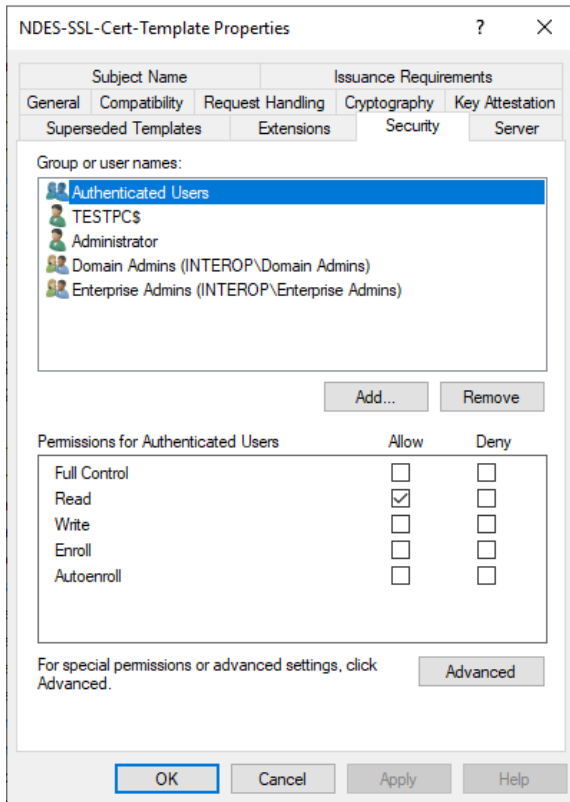
8. Return to the **Certification Authority** window, right-click **Certificate Templates**, and select **New > Certificate Template to Issue**.

9. Select the certificate template that you created earlier, then select **OK**.
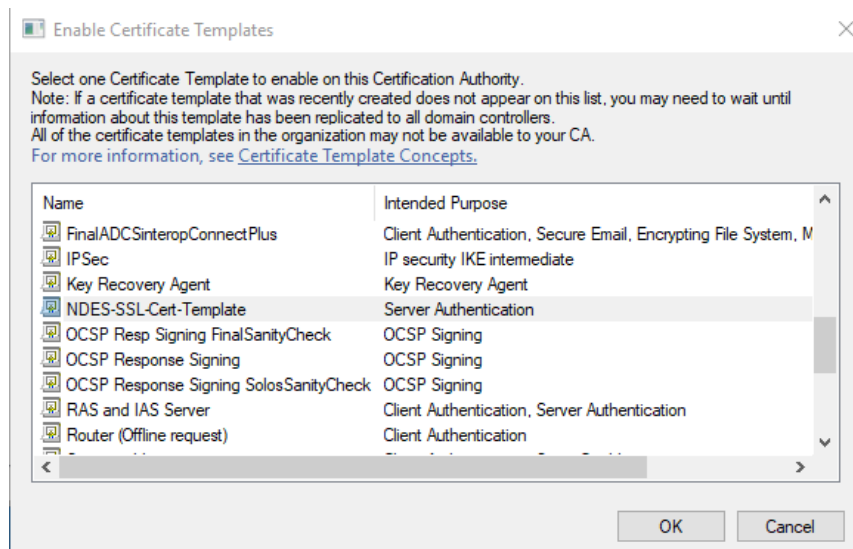
10. Run the following command to generated the certificate:

```
certreq -submit -attrib "CertificateTemplate:<New-Template-Name>" <Path-to-request.req>
```
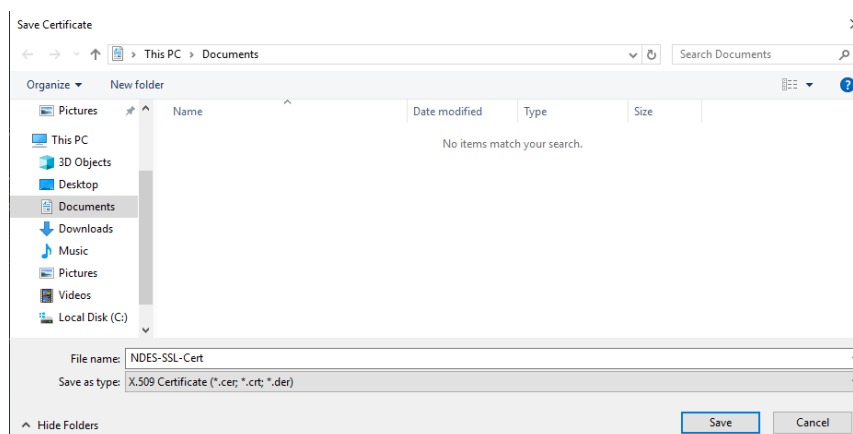
Partial output before executing the following steps:

```
>certreq -submit -attrib "CertificateTemplate:NDES-SSL-Cert-Template" NDES-SSL-Cert.req NDES-SSL-Cert.cer
Active Directory Enrollment Policy
  {96E14557-DDD4-48BD-BE1A-AA453F20D859}
  ldap:
```

11. Select the CA server from the **Certification Authority List** dialog, then select **OK**. Look for a cog icon which may be flashing on the Taskbar. Present the OCS and enter the passphrase, or enter the Softcard passphrase.
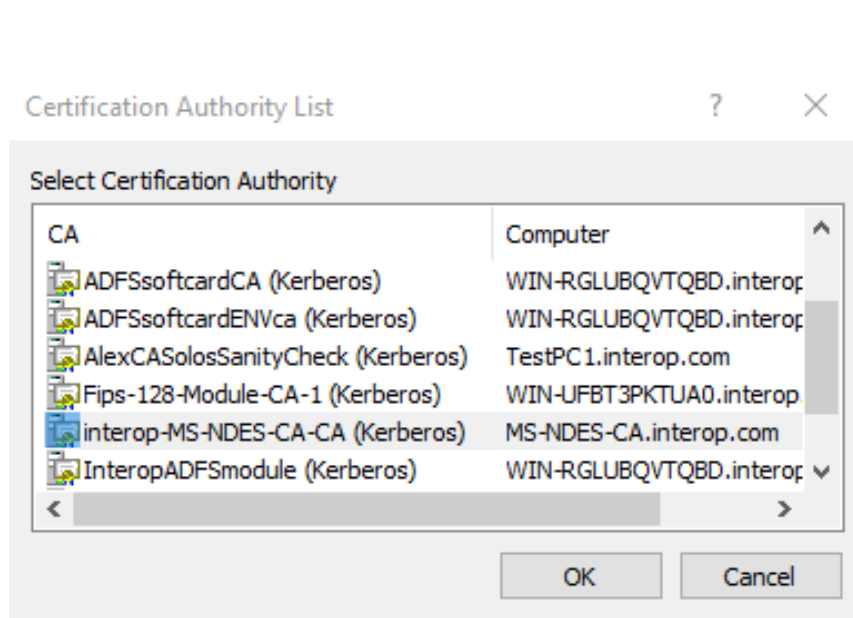
12. Enter the name for the certificate generated on the **Save Certificate** dialog.

The final output is shown below:

```
>certreq -submit -attrib "CertificateTemplate:NDES-SSL-Cert-Template" NDES-SSL-Cert.req NDES-SSL-Cert.cer
Active Directory Enrollment Policy
  {96E14557-DDD4-48BD-BE1A-AA453F20D859}
  ldap:
RequestId: 11
RequestId: "11"
```

13. Copy the above certificate to the NDES server.

Install the certificate on the NDES server, matching it with the private key previously created using the nCipher CSP.

1. Log into the NDES server using the domain name, <domain_name>\Administrator.

2. Run the following command. If you are using OCS or Softcard protection, present the card or enter the Softcard passphrase when prompted.

```
>certreq.exe -accept <Name-of-Certificate>.cer
```

Example output:

```
>certreq -accept NDES-SSL-Cert.cer
Installed Certificate:
  Serial Number: 7c0000000bf544d43dadb23a2f00000000000b
  Subject: CN=ms-ndes-serv.interop.com
  NotBefore: 10/7/2021 12:00 AM
  NotAfter: 10/7/2023 12:10 AM
  Thumbprint: a07344a115b23f7cd903851af3b66884e55aa3ea
```

3. Open `certlm.msc` by right-clicking on the Windows **Start** menu, then select **Run**, type `certlm.msc`, and select **OK**.

4. Expand the **Personal** store on the left pane and then select **Certificates**.

5. Check the certificate installed above is available.
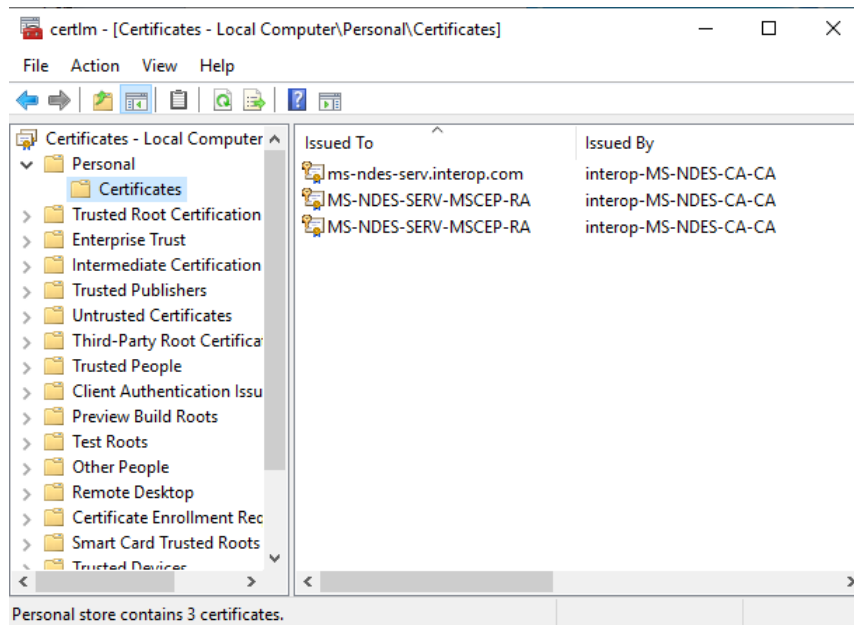
6. Open the IIS manager, expand the server and **Sites** on the **Connections** pane and select **Default Web Site**.

7. Select **Bindings** on the **Actions** pane.

8. Select **Add** on the **Site Bindings** dialog.

9. Select **https** in **Type:** on the **Add Site Binding** dialog. Choose the certificate previously created in **SSL certificate**. Then select **OK** and **Close**.
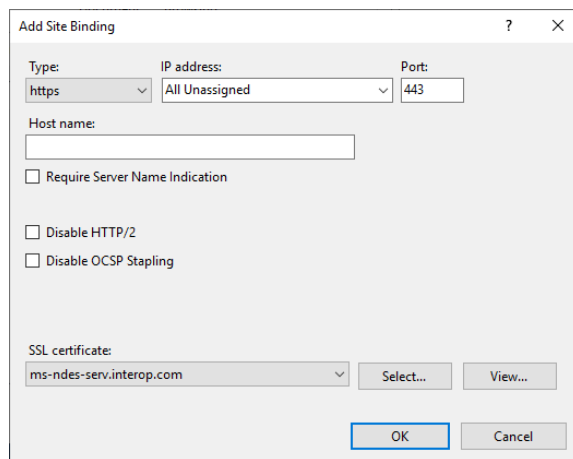
Increase the maximum number of allowed unique passwords generated by the NDES service to 30 before the service needs to be restarted.

1. Log into the NDES server using the domain name, <domain_name>\Administrator.

2. Open **regedit** by right-clicking on the Windows **Start** menu, then select **Run**, type `certlm.msc`, and select **OK**.

3. Navigate to **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\ MSCEP**.

4. Right-click on the right pane and select **New** > **Key** > **DWORD (32-bit)**. Name the key **PasswordMax**.

5. Right-click on the key and select **Modify**. Set **Value data** to 30 on the **Edit DWORD (32-bit) Value** dialog. Then select **OK**.

6. Restart the IIS server. Open the IIS manager, select the server on the **Connections** pane and select **Restart** on the **Actions** pane.

Test access to the NDES web site (secured).

1. Log into the Windows client.

2. Launch the browser and go to the following address: https://<NDES-server-address>/CertSrv/mscep_admin. Log in as <domain-name>\SCEPSvc.
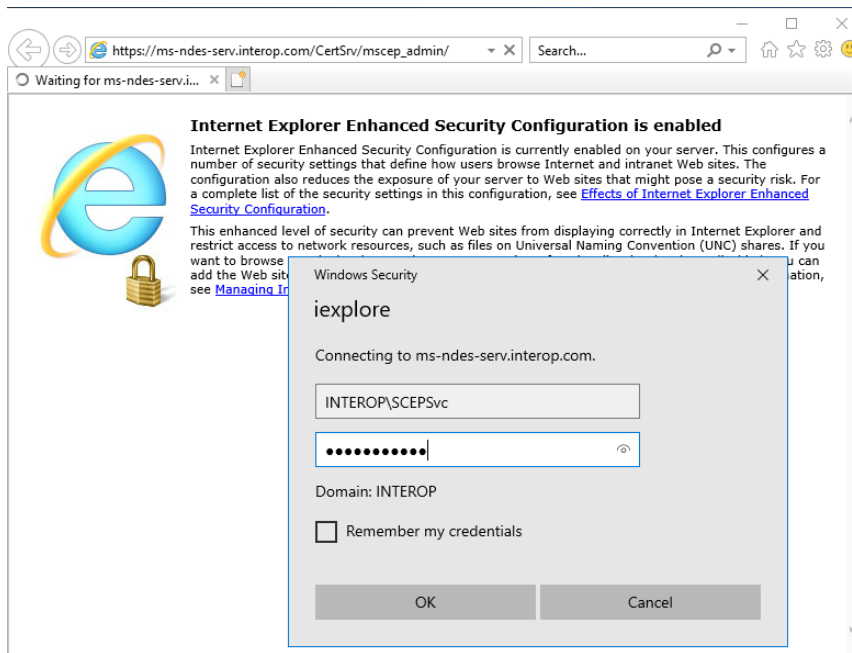
3. Notice the hash value of the CA certificate and the challenge password. Refreshing the browser generates a new challenge password.
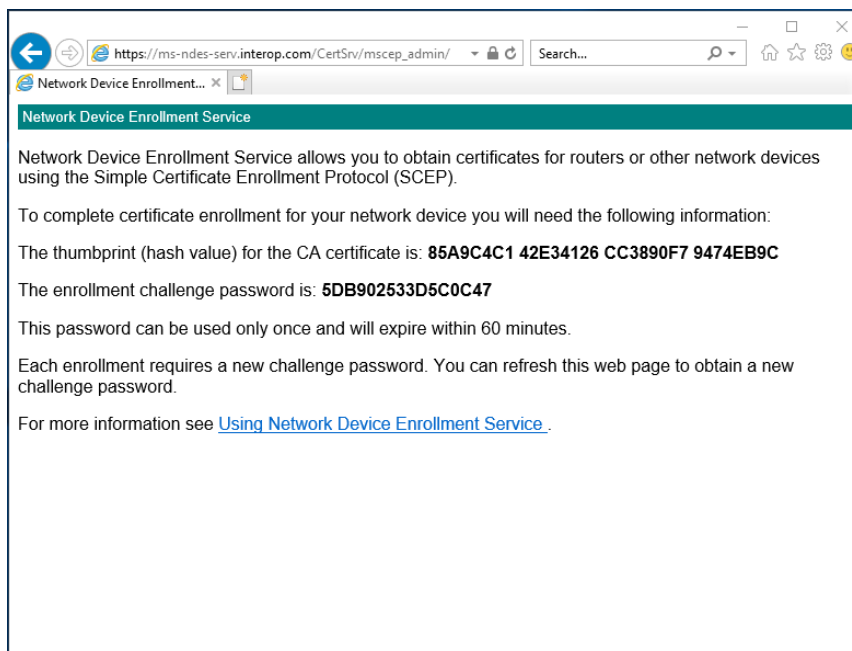
Chapter 3. Troubleshooting

Use the following table to troubleshoot the error messages shown.

Problem	Cause	Resolution
Using the `certreq -new <.req file here>` command returns an Invalid Provider Specified error.	This error occurs when the CSPs are not installed or not set up correctly.	Ensure that the nCipher CNG CSP providers are correctly installed and set. (Do this by running the **CSP Install Wizard** and **CNG Configuration Wizard** under **nCipher** in the **Start** menu).
If using remote admin, the **AD CS Configuration Wizard** does not detect the OCS. `cardpp --examine` shows **TokenSecureChannelError**.	**TokenSecureChannelError** can occasionally be seen when presenting the OCS.	Remove and re-insert the cards until it is picked up by `cardpp` and the **AD CS Configuration Wizard**.