DigiCert® PKI Platform

HSM Installation and Configuration for nShield

August 20, 2020

Legal Notice

The product described in this document is provided by DigiCert, Inc. and distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of DigiCert, Inc. and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. DIGICERT, INC. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The licensed software and documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the licensed software and documentation by the U.S. Government shall be solely in accordance with the terms of this documentation.

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
https://www.digicert.com/

Table of Contents

Introduction

This document describes the installation and configuration steps for the nShield Connect HSM that DigiCert PKI Enterprise Gateway and Autoenrollment server uses.

Revision History

No.	Date	Summary
1.	2019/05/10	Create a new entry
2.	2019/08/30	The algorithm of signature for PKCS#10(CSR) has been changed from SHA1 to SHA256.
3.	2019/11/20	Provider Type changed to 0 as Provider Type is not defined for KSP
4.	2020/03/23	Added support for: • Strict FIPS 140-2 Level 3 enabled • OCS – 1 of 3 with passphrase for CNG • OCS is set in non-persistent mode
5.	2020/08/20	Removed OCS protection related section.

Supported HSMs

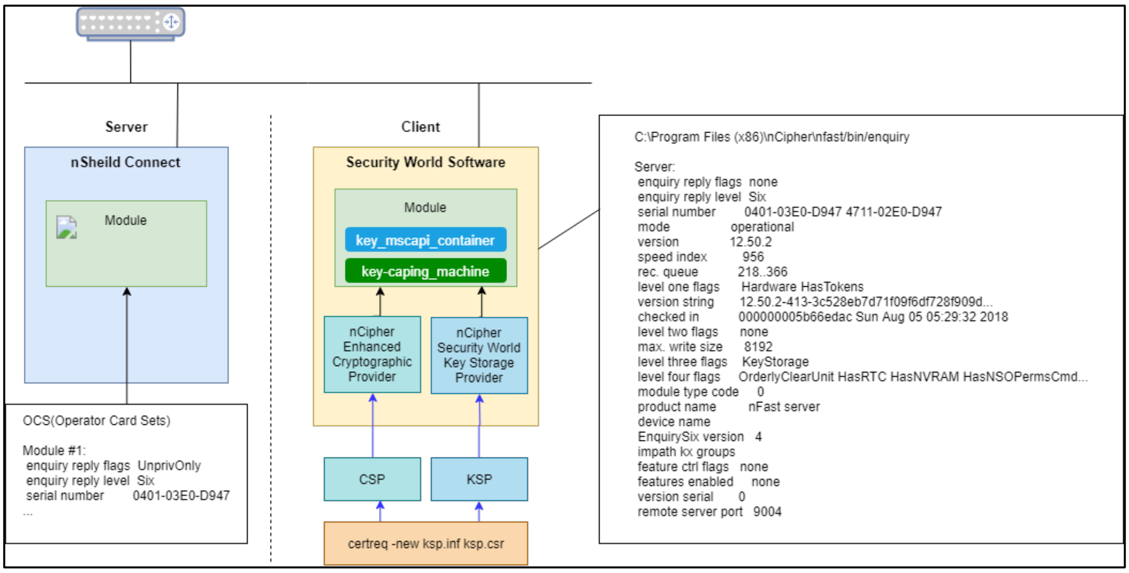
HSM Type	Client Version	Software Version	Firmware Version

nShield Connect HSM	12.50.2	12.50.2	The following is the output of enquiry (or nfdiag) command
			`nfast server: 2.103.13`
			`module: 3.4.2`

nShield Connect HSM • Strict FIPS 140-2 Level 3 enabled • Module protection for CSP and CNG	12.50.2	12.50.2	2.61.2

nShield Connect HSM

nShield Connect is network HSM, which allows you to create a module (Operator Card Sets) to store a key. Security World Software can access the partition of the HSM through secure channel.

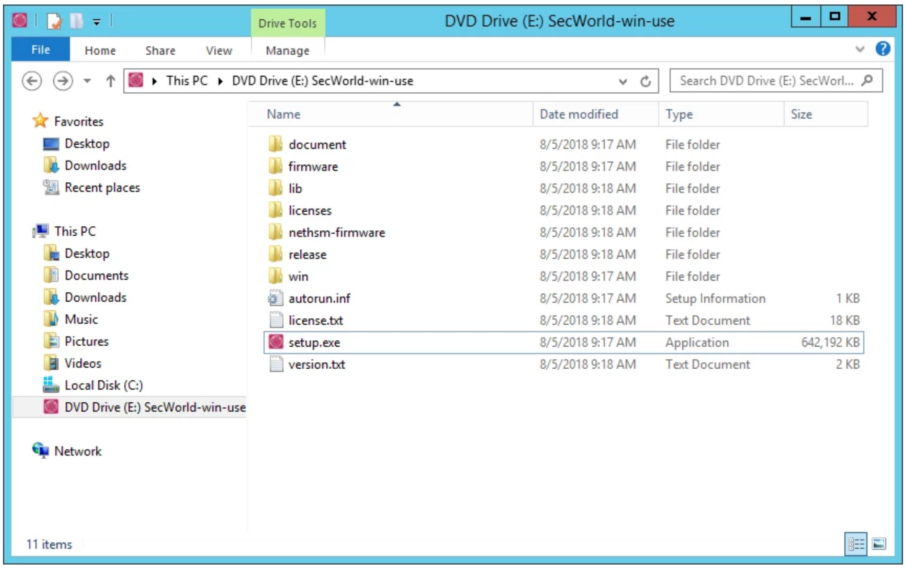

Server
nSheild Connect
Module
Client
Security World Software
Module
key_mscapi_container
key-caping_machine
nCipher Enhanced Cryptographic Provider
nCipher Security World Key Storage Provider
CSP
KSP
certreq -new ksp.inf ksp.csr

```
OCS(Operator Card Sets)

Module #1:
 enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        0401-03E0-D947
...
```

```
C:\Program Files (x86)\nCipher\nfast/bin/enquiry

Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        0401-03E0-D947 4711-02E0-D947
 mode                 operational
 version              12.50.2
 speed index          956
 rec. queue           218..366
 level one flags      Hardware HasTokens
 version string       12.50.2-413-3c528eb7d71f09f6df728f909d...
 checked in           000000005b66edac Sun Aug 05 05:29:32 2018
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd...
 module type code     0
 product name         nFast server
 device name
 EnquirySix version   4
 impath kx groups
 feature ctrl flags   none
 features enabled     none
 version serial       0
 remote server port   9004
```

Install Security World Software

1. Extract or mount the iso image.

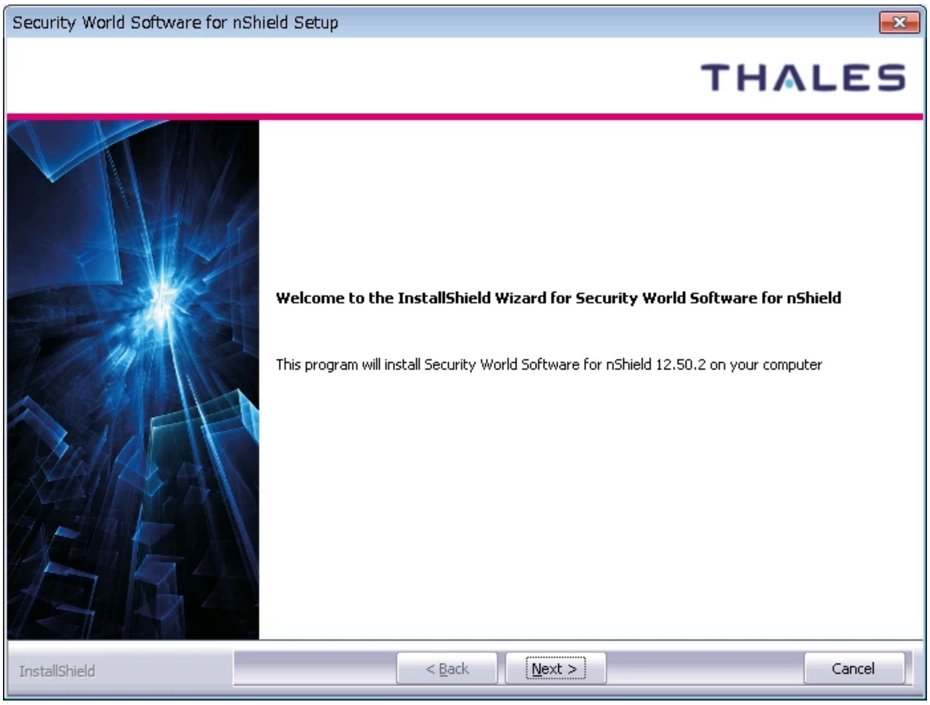


Name	Date modified	Type	Size
document	8/5/2018 9:17 AM	File folder	
firmware	8/5/2018 9:17 AM	File folder	
lib	8/5/2018 9:18 AM	File folder	
licenses	8/5/2018 9:18 AM	File folder	
nethsm-firmware	8/5/2018 9:18 AM	File folder	
release	8/5/2018 9:18 AM	File folder	
win	8/5/2018 9:17 AM	File folder	
autorun.inf	8/5/2018 9:17 AM	Setup Information	1 KB
license.txt	8/5/2018 9:18 AM	Text Document	18 KB
setup.exe	8/5/2018 9:17 AM	Application	642,192 KB
version.txt	8/5/2018 9:18 AM	Text Document	2 KB

NOTE: If you try to upgrade the client software, the old version must be uninstalled. After uninstallation, the system requires to reboot the computer.

Even if you uninstall the old version, you do not have to configure the client software again because the HSM has already configured the client.

2. Run "**setup.exe**" as Administrator.

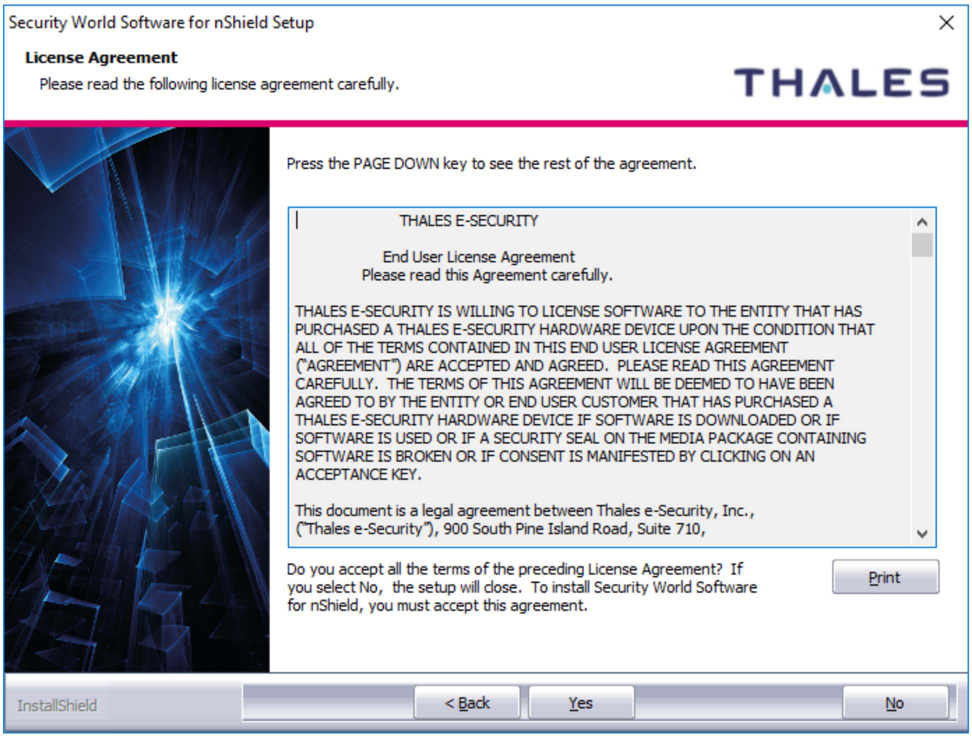


Security World Software for nShield Setup

Welcome to the InstallShield Wizard for Security World Software for nShield

This program will install Security World Software for nShield 12.50.2 on your computer

3. Accept the Software License Agreement.



Security World Software for nShield Setup

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

THALES E-SECURITY

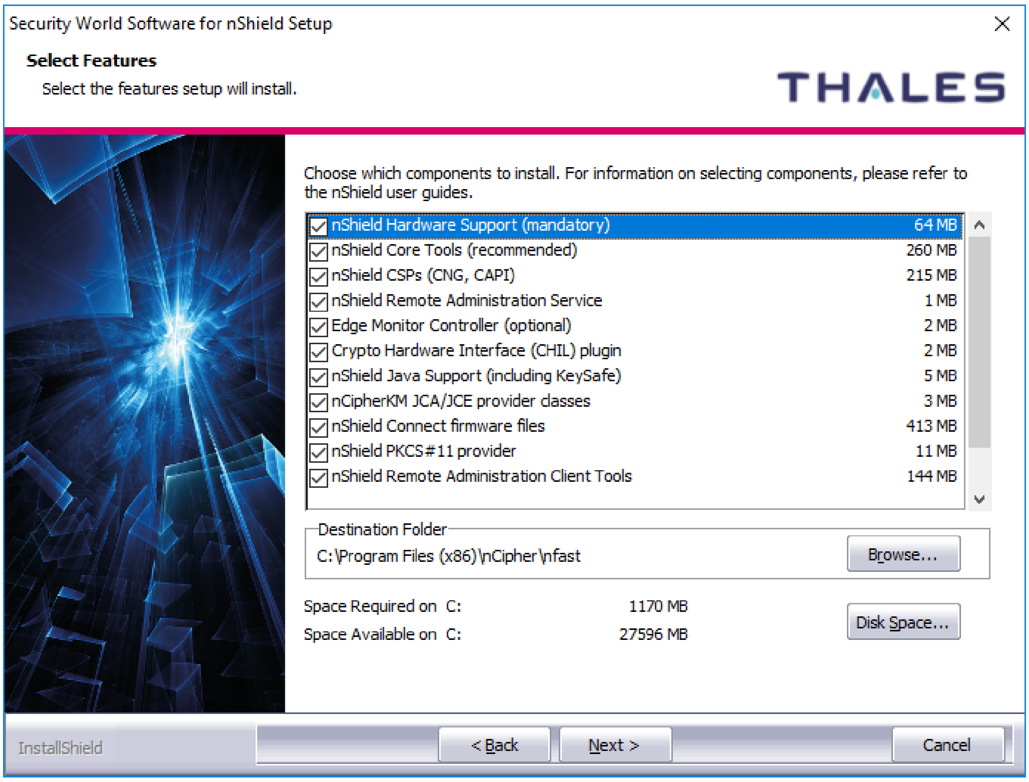
End User License Agreement
Please read this Agreement carefully.

THALES E-SECURITY IS WILLING TO LICENSE SOFTWARE TO THE ENTITY THAT HAS PURCHASED A THALES E-SECURITY HARDWARE DEVICE UPON THE CONDITION THAT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT ("AGREEMENT") ARE ACCEPTED AND AGREED. PLEASE READ THIS AGREEMENT CAREFULLY. THE TERMS OF THIS AGREEMENT WILL BE DEEMED TO HAVE BEEN AGREED TO BY THE ENTITY OR END USER CUSTOMER THAT HAS PURCHASED A THALES E-SECURITY HARDWARE DEVICE IF SOFTWARE IS DOWNLOADED OR IF SOFTWARE IS USED OR IF A SECURITY SEAL ON THE MEDIA PACKAGE CONTAINING SOFTWARE IS BROKEN OR IF CONSENT IS MANIFESTED BY CLICKING ON AN ACCEPTANCE KEY.

This document is a legal agreement between Thales e-Security, Inc., ("Thales e-Security"), 900 South Pine Island Road, Suite 710,

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install Security World Software for nShield, you must accept this agreement.

4. Select the components and the destination and click **Next**.



Security World Software for nShield Setup

Select Features

Select the features setup will install.

Choose which components to install. For information on selecting components, please refer to the nShield user guides.

☑ nShield Hardware Support (mandatory)	64 MB
☑ nShield Core Tools (recommended)	260 MB
☑ nShield CSPs (CNG, CAPI)	215 MB
☑ nShield Remote Administration Service	1 MB
☑ Edge Monitor Controller (optional)	2 MB
☑ Crypto Hardware Interface (CHIL) plugin	2 MB
☑ nShield Java Support (including KeySafe)	5 MB
☑ nCipherKM JCA/JCE provider classes	3 MB
☑ nShield Connect firmware files	413 MB
☑ nShield PKCS#11 provider	11 MB
☑ nShield Remote Administration Client Tools	144 MB

Destination Folder

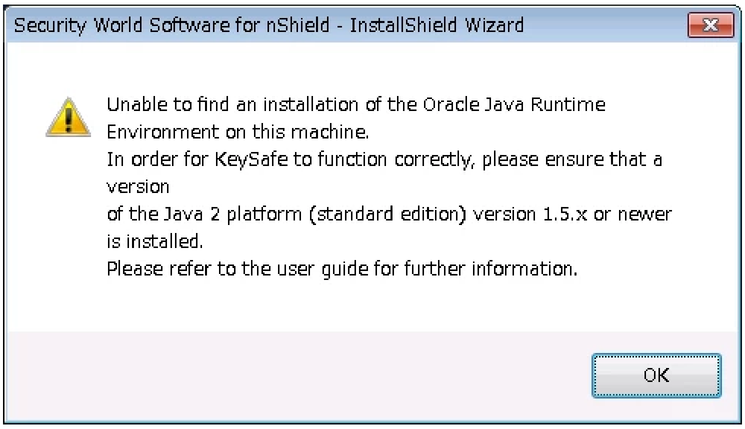
C:\Program Files (x86)\nCipher\nfast

Space Required on C: 1170 MB

Space Available on C: 27596 MB

- Select all the components by default.
- Change the destination folder if you want.
- Click **Next**.

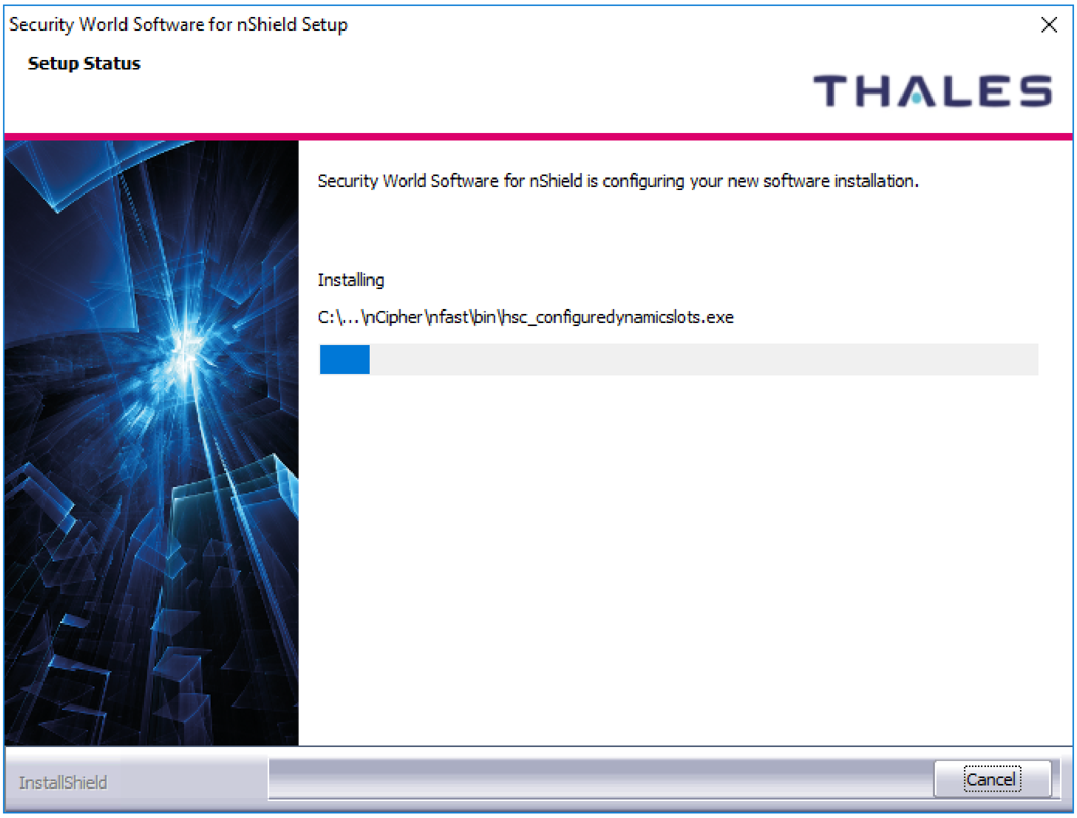
NOTE: When **Next** is clicked, the following notification is displayed.



Security World Software for nShield - InstallShield Wizard

Unable to find an installation of the Oracle Java Runtime Environment on this machine.
In order for KeySafe to function correctly, please ensure that a version
of the Java 2 platform (standard edition) version 1.5.x or newer is installed.
Please refer to the user guide for further information.

5. Wait for the completion.



Security World Software for nShield Setup

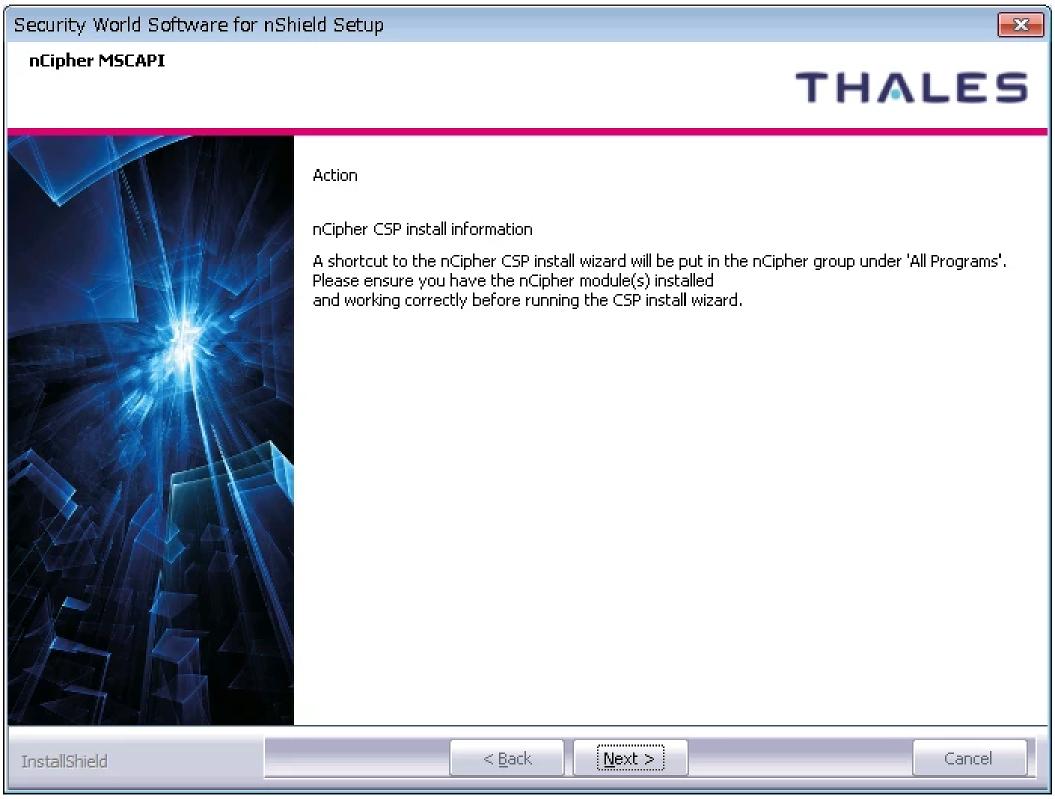
Setup Status

Security World Software for nShield is configuring your new software installation.

Installing

C:\...\nCipher\nfast\bin\hsc_configuredynamicslots.exe

6. Create shortcut for CSP and click **Next**.



Security World Software for nShield Setup

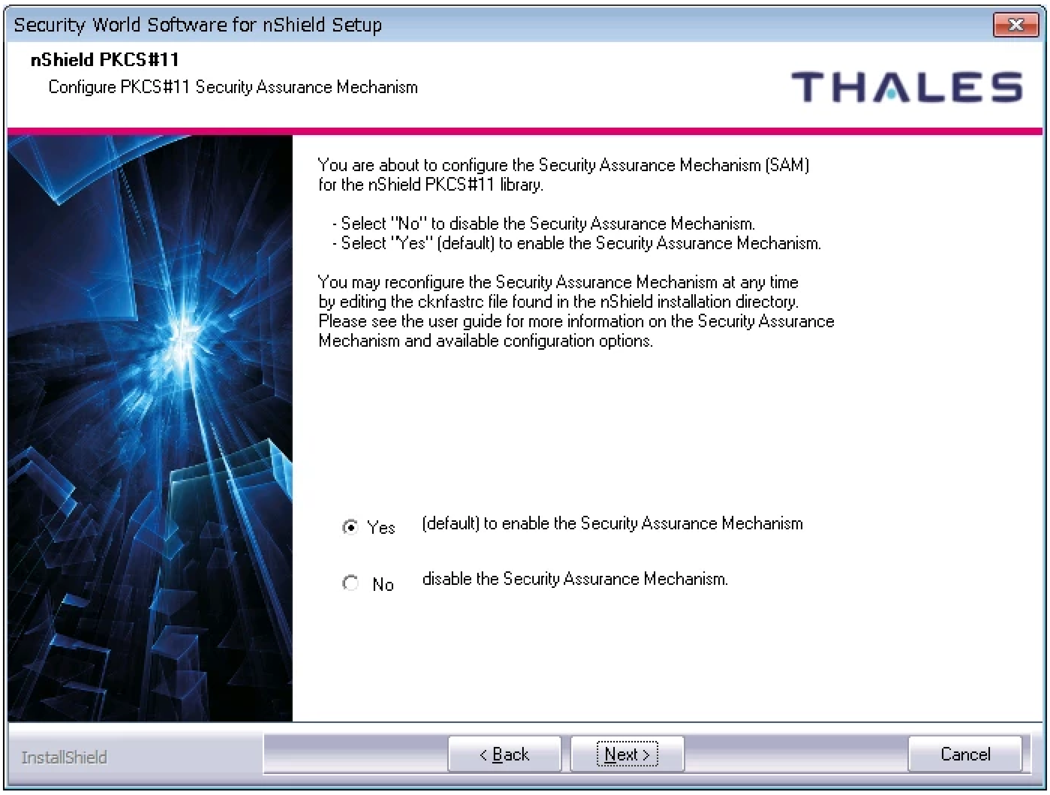
nCipher MSCAPI

Action

nCipher CSP install information

A shortcut to the nCipher CSP install wizard will be put in the nCipher group under 'All Programs'.
Please ensure you have the nCipher module(s) installed
and working correctly before running the CSP install wizard.

7. Install nShield PKCS#11and click **Next**.



Security World Software for nShield Setup

nShield PKCS#11

Configure PKCS#11 Security Assurance Mechanism

You are about to configure the Security Assurance Mechanism (SAM) for the nShield PKCS#11 library.

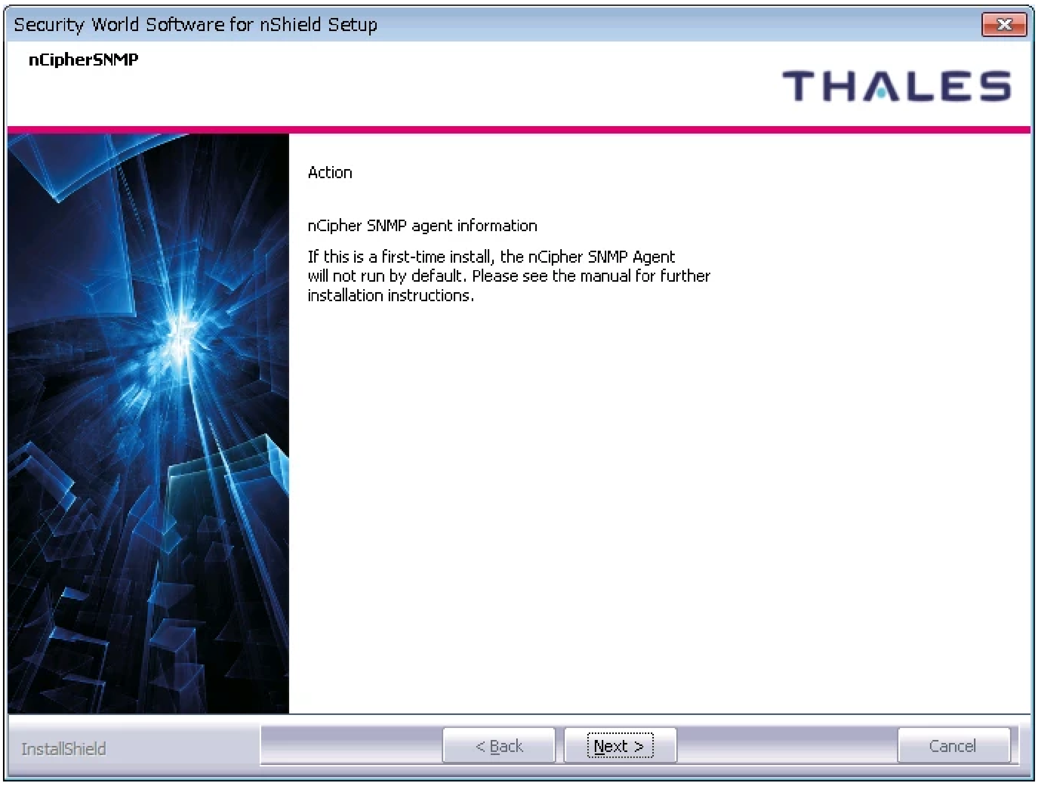
- Select "No" to disable the Security Assurance Mechanism.
- Select "Yes" (default) to enable the Security Assurance Mechanism.

You may reconfigure the Security Assurance Mechanism at any time by editing the cknfastrc file found in the nShield installation directory. Please see the user guide for more information on the Security Assurance Mechanism and available configuration options.

● Yes (default) to enable the Security Assurance Mechanism

○ No disable the Security Assurance Mechanism.

8. Install SNMP Agent and click **Next.**



Security World Software for nShield Setup

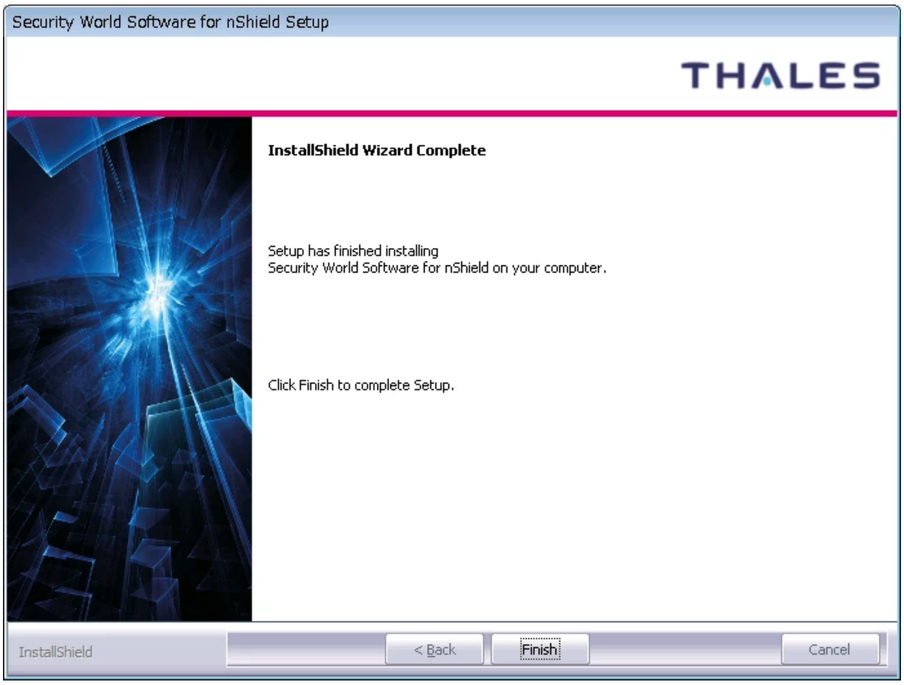
nCipherSNMP

Action

nCipher SNMP agent information

If this is a first-time install, the nCipher SNMP Agent will not run by default. Please see the manual for further installation instructions.

9. Installation is now complete. Click **Finish**.


Security World Software for nShield Setup

InstallShield Wizard Complete

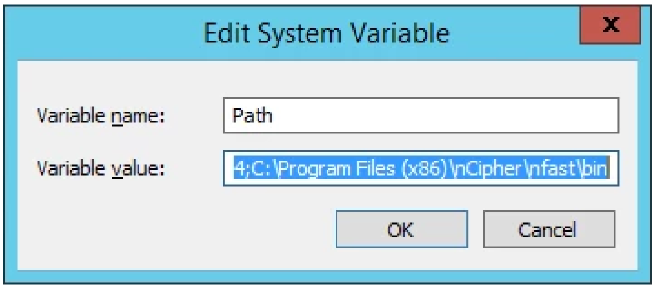
Setup has finished installing
Security World Software for nShield on your computer.

Click Finish to complete Setup.

NOTE: After uninstallation, several files of the old software remains at the Program folders under "Programs and Features". You need to manually remove the files for the installation to proceed.

Configure Security World Software

1. Add the path of executable file into environment variables.


Edit System Variable

Variable name: Path

Variable value: 4;C:\Program Files (x86)\nCipher\nfast\bin

2. Prepare to configure the client software.

Each client computer must be configured to use the internal security module of your nShield Connect. There are two methods for achieving this:

- Enrolling the client with the configuration file.
- Enrolling the client with command-line utilities.

3. Check if the tool works.

The **nethsmenroll** command-line utility edits the client hardserver's configuration file to add the specified nShield Connect. For more information about the options available to use with **nethsmenroll**, read the following section Client configuration utilities, or run the command:

```
nethsmenroll -help
```

4. Obtain the HSM ESN and HKNETI information.

   Obtain the following information about the HSM before you set up an RFS for the first time:

   - The IP Address
   - The electronic serial number (ESN)
   - The hash of the KNETI key (HKNETI)

   The KNETI key authenticates the HSM to clients. It is generated when the HSM is first initialized from factory state.

   To retrieve the nShield Connect's ESN and HKNETI, run the command:

   ```
   anonkneti <Unit IP>
   ```

   The example output of the command is as follows;

   ```
   >anonkneti.exe 10.204.153.52
   0401-03E0-D947 18fd6da2186bd778259d31bd63cee09a01b68794
   ```

5. Register the configuration of the client into HSM.

   The nethsmenroll command-line utility edits the client hardserver's configuration file to add the specified nShield Connect.
   If you are enrolling the client without a nToken, run the command:

   ```
   > nethsmenroll [Options] --privileged < Unit IP> < Unit ESN> < Unit KNETI
   HASH>
   ```

   An example output is as follows:

   ```
   > nethsmenroll -p <SERVER-IP> <ESN> <KNETIHASH>
   OK configuring hardserver's nethsm imports
   ```

NOTE: The following is an output of the command if the entry that you want to add already exists.

```
> nethsmenroll -p 10.204.153.52 0401-03E0-D947
18fd6da2186bd778259d31bd63cee09a01b68794

nethsmenroll: an entry with ESN 0401-03E0-D947 already exists; use `--force' to
overwrite it
```

6. Startup config-server.

   The config-serverstartup command-line utility automatically edits the [server_startup] section in the local hardserver configuration file in order to enable TCP ports for Java and KeySafe. Any fields for which values are not specified remain unchanged. After making any changes you are prompted to restart the hardserver.

   ```
   > config-serverstartup [OPTIONS]
   ```

7. Test the installation.

   To test the installation and configuration, follow these steps:

   - Log in on the client computer as a regular user and open a command window.
   - Run the command:

   ```
   > enquiry
   ```

   A successful enquiry command returns an output of the following form:

   ```
   Server:
   enquiry reply flags none
   enquiry reply level Six
   serial number ####-####-####
   mode operational
   version #-#-#
   speed index ######
   rec. queue ####..####
   ---
   version serial #
   remote server port ####
   Module ##:
   enquiry reply flags none
   enquiry reply level Six
   serial number ####-####-####
   mode operational
   version #-#-#
   speed index #####
   rec. queue ##..###
   ---
   rec. LongJobs queue ##
   SEE machine type PowerPCELF
   supported KML types DSAp1024s160 DSAp3072s256
   hardware status 0
   ```

NOTE: If the enquiry command says that the unit is not found:

Restart the client computer.

Re-run the enquiry command.

8. Configure RFS synchronization.

The remote file system (RFS) contains the master copy of the HSM Security World data for backup purposes. The RFS can be located on either a client or another network-accessible computer where the Security World Software is installed. If the RFS is on a client, the same file structure also contains the configuration files for that client.

```
C:\Users\Administrator> rfs-sync.exe --setup --no-authenticate <RFS-IP>
No current RFS synchronization configuration.
Configuration successfully written; new config details:
Using RFS at <RFS-IP>:9004: not authenticating.

C:\Users\Administrator> rfs-sync.exe --update
Starting synchronisation, task ID 5ca6fa8a.32f596d69d1bb3ca
Updated (new) card_b5310850ab6c82e1605382c7b68b183cda60d13a_1
Updated (new) card_b5310850ab6c82e1605382c7b68b183cda60d13a_2
Updated (new) card_b5310850ab6c82e1605382c7b68b183cda60d13a_3
...
Updated (new) module_0401-03E0-D947
Updated (new) module_4711-02E0-D947
Updated (new) world
Finished synchronisation: 53 files updated, 0 committed.


C:\Users\Administrator> rfs-sync -c
Starting synchronisation, task ID 5ca48468.764b879a080c7eca
This client does not have commit permission to the RFS;you must run 'rfs-
setup -
-gang-client' on the RFS first.
```

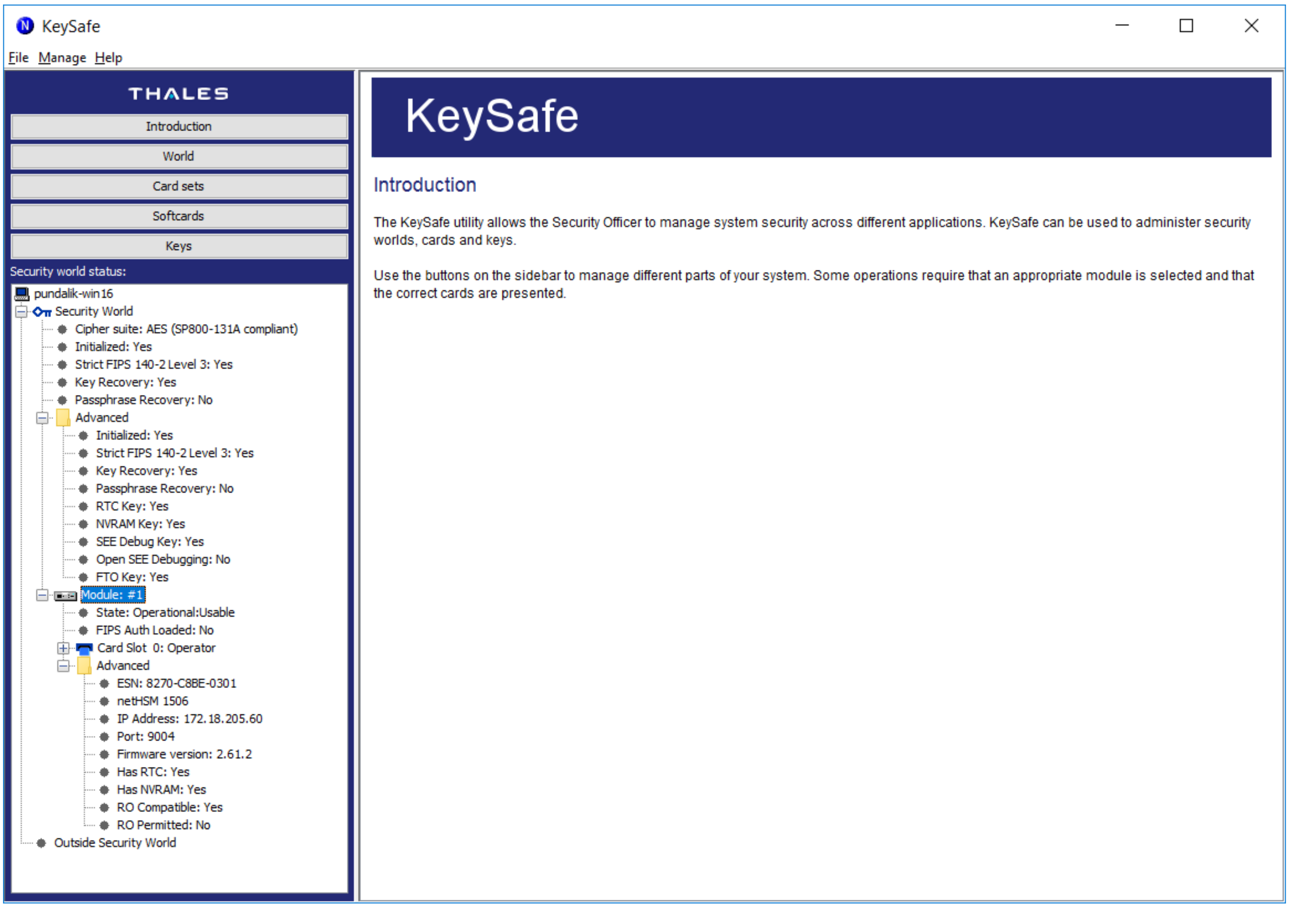
NOTE: The RFS synchronization port is 9004.

After the setup, the following command must be executed:

```
rfs-sync.exe –update
```

9. Check status through KeySafe. Run the following command.

```
C:\Program Files (x86)\nCipher\nfast\bin\ksafe.exe
```



KeySafe

Introduction

The KeySafe utility allows the Security Officer to manage system security across different applications. KeySafe can be used to administer security worlds, cards and keys.

Use the buttons on the sidebar to manage different parts of your system. Some operations require that an appropriate module is selected and that the correct cards are presented.

Security world status:

- pundalik-win16
  - Security World
    - Cipher suite: AES (SP800-131A compliant)
    - Initialized: Yes
    - Strict FIPS 140-2 Level 3: Yes
    - Key Recovery: Yes
    - Passphrase Recovery: No
    - Advanced
      - Initialized: Yes
      - Strict FIPS 140-2 Level 3: Yes
      - Key Recovery: Yes
      - Passphrase Recovery: No
      - RTC Key: Yes
      - NVRAM Key: Yes
      - SEE Debug Key: Yes
      - Open SEE Debugging: No
      - FTO Key: Yes
    - Module: #1
      - State: Operational:Usable
      - FIPS Auth Loaded: No
      - Card Slot 0: Operator
      - Advanced
        - ESN: 8270-C8BE-0301
        - netHSM 1506
        - IP Address: 172.18.205.60
        - Port: 9004
        - Firmware version: 2.61.2
        - Has RTC: Yes
        - Has NVRAM: Yes
        - RO Compatible: Yes
        - RO Permitted: No
  - Outside Security World

NOTE: Please find the details of KeySafe in "nShield Connect User Guide for Windows"

Configure HA (High Availability)

For example, there are several hardservers (e.g. Server-A, Server-B). To configure HA, add all the hardservers as follows:

1. Obtain the HSM ESN and HKNETI information.

   To retrieve the nShield Connect's ESN and HKNETI, run the command:

   ```
   anonkneti <Unit IP>
   ```

   The example of output of the command is as follows:

   ```
   >anonkneti.exe <Server-A IP>
   0401-03E0-D947 18fd6da2186bd778259d31bd63cee09a01b68794
   >anonkneti.exe <Server-B IP>
   4711-02E0-D947 c4405efd401b3719c109cde104832e3eec18376c
   ```

2. Add all the hardservers.

The nethsmenroll command-line utility edits the client hardserver's configuration file to add the specified nShield Connect.

If you are enrolling the client without an nToken, run the command:

```
> nethsmenroll [Options] --privileged < Unit IP> < Unit ESN> < Unit KNETI
HASH>
```

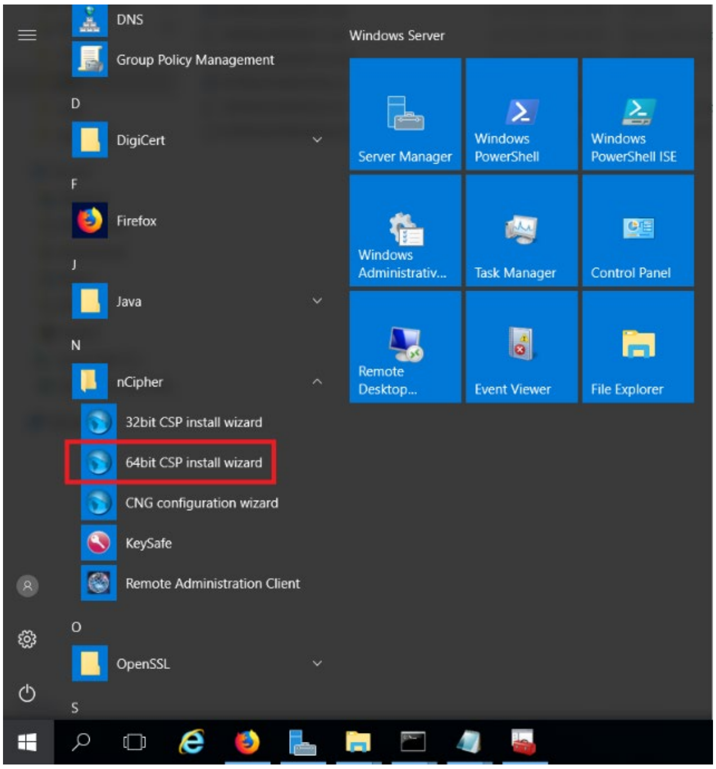
The example outputs are as follows;

```
> nethsmenroll -p <Server-A IP> 0401-03E0-D947
18fd6da2186bd778259d31bd63cee09a01b68794
OK configuring hardserver's nethsm imports
> nethsmenroll -p <Server-B IP> 4711-02E0-D947
c4405efd401b3719c109cde104832e3eec18376c
OK configuring hardserver's nethsm imports
```

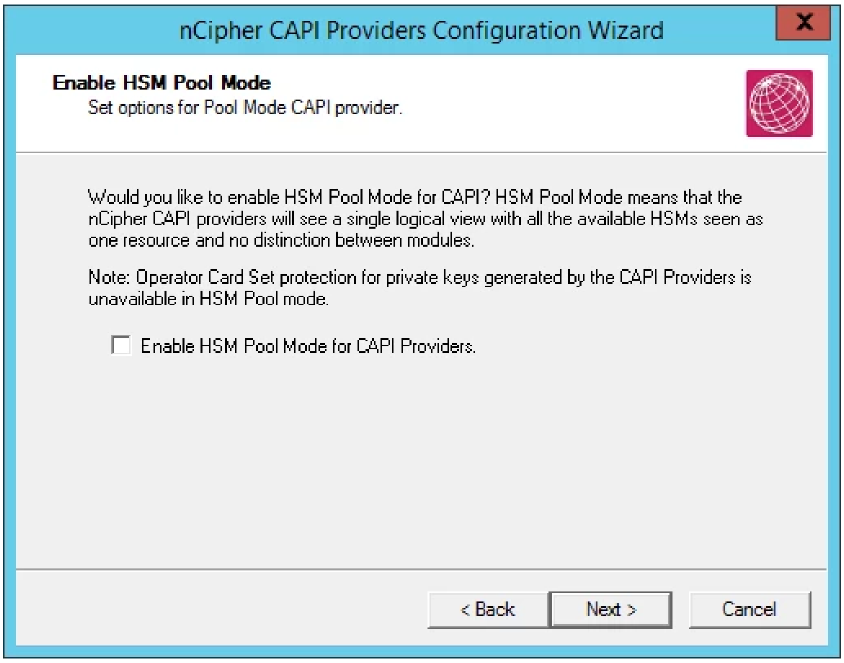
Configure CSP (Module protection)

NOTE: Please note that for the deployment of the Autoenrollment Server, you need to Configure CSP.

1. Go to **Start**-> **nCipher** and run CSP Install wizard (64bit).



2. On Enable HSM Pool Mode, click **Next**.



nCipher CAPI Providers Configuration Wizard

Enable HSM Pool Mode

Set options for Pool Mode CAPI provider.

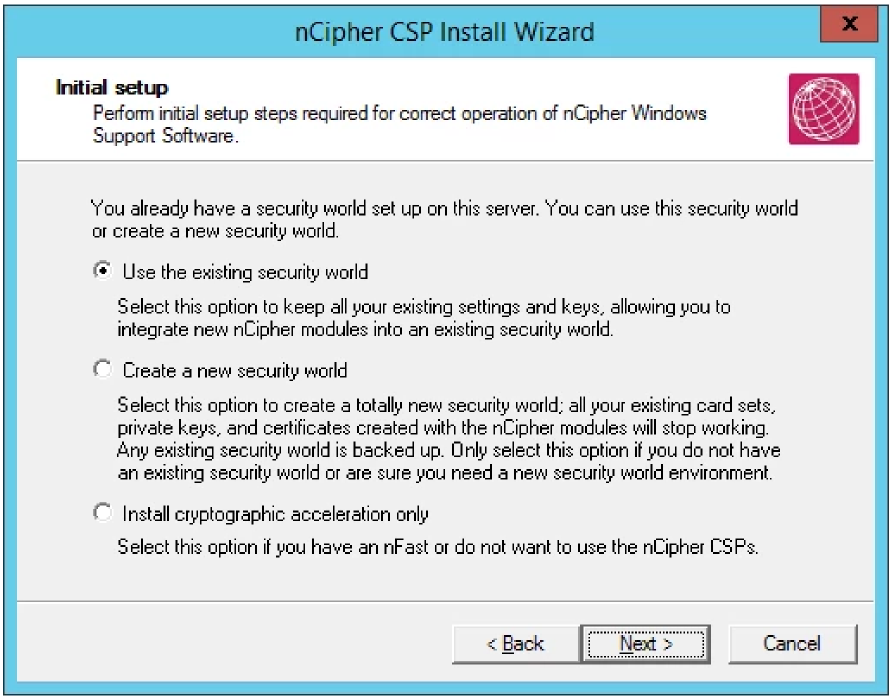
Would you like to enable HSM Pool Mode for CAPI? HSM Pool Mode means that the nCipher CAPI providers will see a single logical view with all the available HSMs seen as one resource and no distinction between modules.

Note: Operator Card Set protection for private keys generated by the CAPI Providers is unavailable in HSM Pool mode.

□ Enable HSM Pool Mode for CAPI Providers.

NOTE: Do not select the "Enable HSM Pool Mode for CAPI Providers" checkbox.

3. On Initial setup dialog box, click **Next**.



nCipher CSP Install Wizard

Initial setup

Perform initial setup steps required for correct operation of nCipher Windows Support Software.

You already have a security world set up on this server. You can use this security world or create a new security world.

● Use the existing security world

Select this option to keep all your existing settings and keys, allowing you to integrate new nCipher modules into an existing security world.

○ Create a new security world

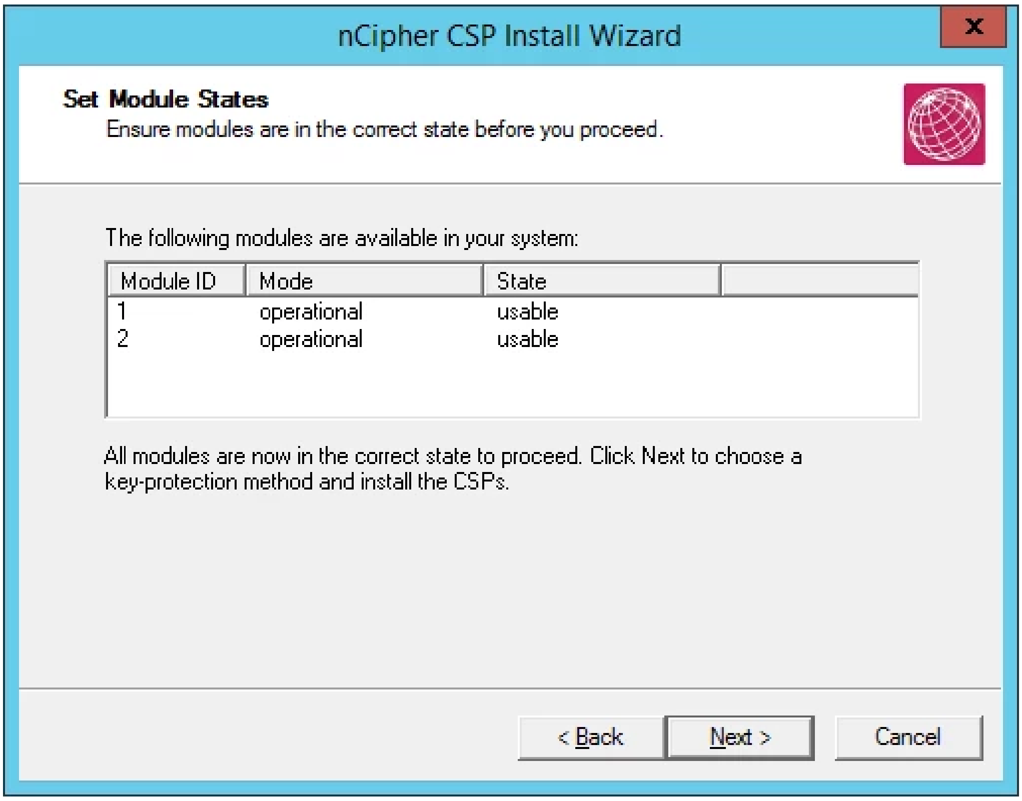
Select this option to create a totally new security world; all your existing card sets, private keys, and certificates created with the nCipher modules will stop working. Any existing security world is backed up. Only select this option if you do not have an existing security world or are sure you need a new security world environment.

○ Install cryptographic acceleration only

Select this option if you have an nFast or do not want to use the nCipher CSPs.

NOTE: The first one (**Use** the **existing security world**) must be selectable. If not, please check the configuration of module. (eg rfs-sync).

4. On Set Module States dialog box, click **Next**.



nCipher CSP Install Wizard

Set Module States

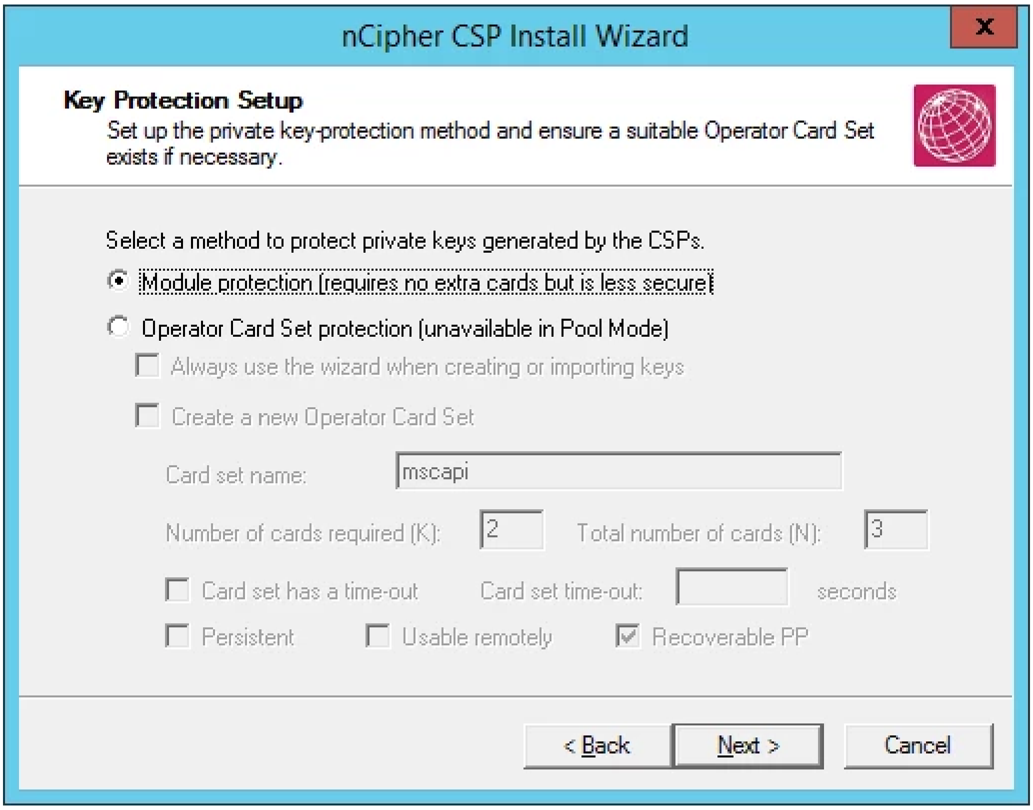
Ensure modules are in the correct state before you proceed.

The following modules are available in your system:

Module ID	Mode	State	
1	operational	usable	
2	operational	usable	

All modules are now in the correct state to proceed. Click Next to choose a key-protection method and install the CSPs.

5. On the Key Protection Setup dialog box, click **Next**.



nCipher CSP Install Wizard

Key Protection Setup

Set up the private key-protection method and ensure a suitable Operator Card Set exists if necessary.

Select a method to protect private keys generated by the CSPs.

● Module protection (requires no extra cards but is less secure)

○ Operator Card Set protection (unavailable in Pool Mode)

□ Always use the wizard when creating or importing keys

□ Create a new Operator Card Set

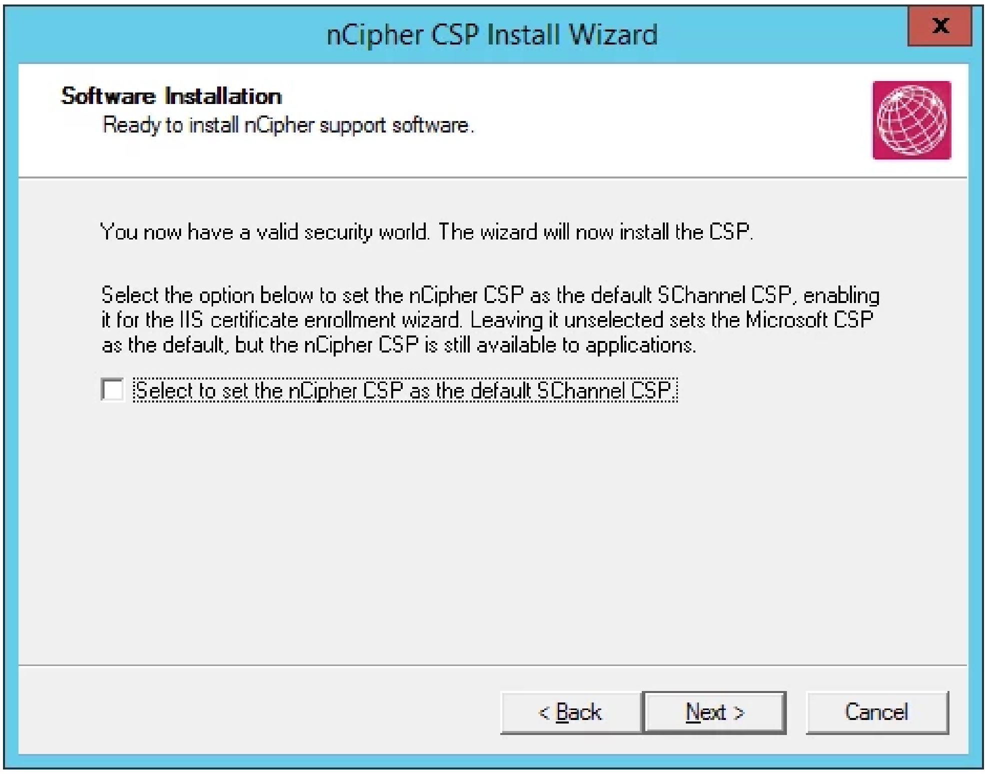
Card set name: mscapi

Number of cards required (K): 2 Total number of cards (N): 3

□ Card set has a time-out Card set time-out: seconds

□ Persistent □ Usable remotely ☑ Recoverable PP

6. On the Software Installation dialog box, click **Next**.



nCipher CSP Install Wizard

Software Installation

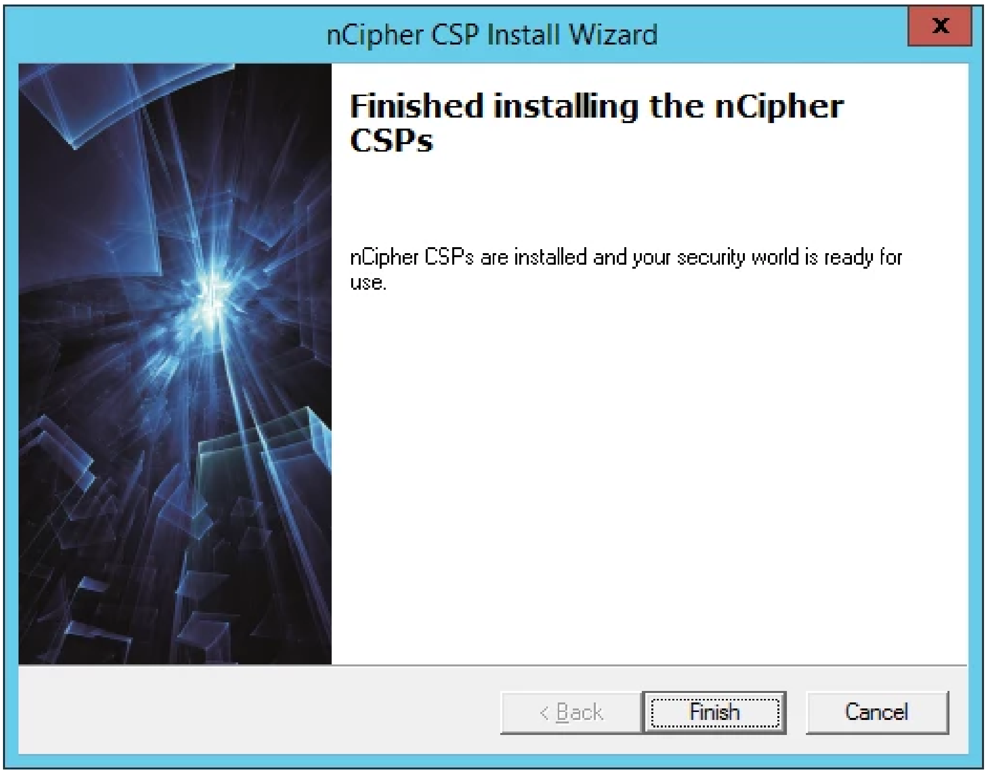
Ready to install nCipher support software.

You now have a valid security world. The wizard will now install the CSP.

Select the option below to set the nCipher CSP as the default SChannel CSP, enabling it for the IIS certificate enrollment wizard. Leaving it unselected sets the Microsoft CSP as the default, but the nCipher CSP is still available to applications.

□ Select to set the nCipher CSP as the default SChannel CSP.

7. Click **Finish**.



nCipher CSP Install Wizard

Finished installing the nCipher CSPs

nCipher CSPs are installed and your security world is ready for use.

8. Confirm the CSP Providers for nCipher.

```
C:\Users\Administrator>certutil -csplist
Provider Name: Microsoft Base Cryptographic Provider v1.0
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
Provider Type: 13 - PROV_DSS_DH

Provider Name: Microsoft Base DSS Cryptographic Provider
Provider Type: 3 - PROV_DSS

Provider Name: Microsoft Base Smart Card Crypto Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft DH SChannel Cryptographic Provider
Provider Type: 18 - PROV_DH_SCHANNEL

Provider Name: Microsoft Enhanced Cryptographic Provider v1.0
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Enhanced DSS and Diffie-Hellman Cryptographic
Provider
Provider Type: 13 - PROV_DSS_DH

Provider Name: Microsoft Enhanced RSA and AES Cryptographic Provider
Provider Type: 24 - PROV_RSA_AES

Provider Name: Microsoft RSA SChannel Cryptographic Provider
Provider Type: 12 - PROV_RSA_SCHANNEL

Provider Name: Microsoft Strong Cryptographic Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: nCipher DSS Signature Cryptographic Provider
Provider Type: 3 - PROV_DSS

Provider Name: nCipher Enhanced Cryptographic Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: nCipher Enhanced DSS and Diffie-Hellman Cryptographic Provider
Provider Type: 13 - PROV_DSS_DH

Provider Name: nCipher Enhanced DSS and Diffie-Hellman SChannel Cryptographic
Provider
Provider Type: 18 - PROV_DH_SCHANNEL

Provider Name: nCipher Enhanced RSA and AES Cryptographic Provider
Provider Type: 24 - PROV_RSA_AES

Provider Name: nCipher Enhanced SChannel Cryptographic Provider
Provider Type: 12 - PROV_RSA_SCHANNEL

Provider Name: Microsoft Software Key Storage Provider

Provider Name: Microsoft Platform Crypto Provider
```

```
Microsoft Platform Crypto Provider: The device that is required
by this cryptographic provider is not ready for use.

Provider Name: Microsoft Smart Card Key Storage Provider
CertUtil: -csplist command FAILED: 0x80090030 (-
2146893776 NTE_DEVICE_NOT_READY)

CertUtil: The device that is required by this cryptographic provider is not
ready for use.
```

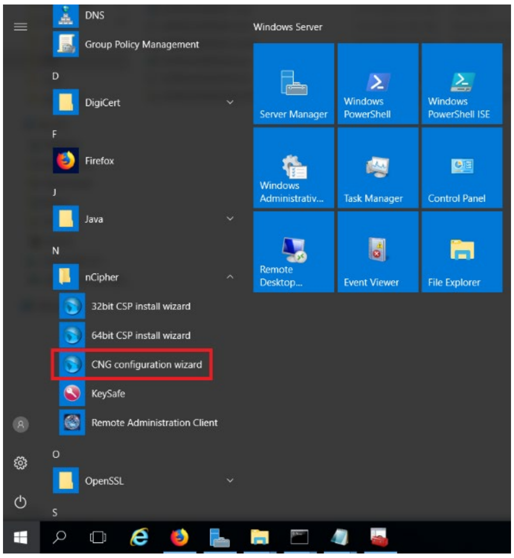
NOTE: You can find the following providers:

nCipher DSS Signature Cryptographic Provider
nCipher Enhanced Cryptographic Provider
nCipher Enhanced DSS and Diffie-Hellman Cryptographic Provider
nCipher Enhanced DSS and Diffie-Hellman SChannel Cryptographic Provider
nCipher Enhanced RSA and AES Cryptographic Provider
nCipher Enhanced SChannel Cryptographic Provider

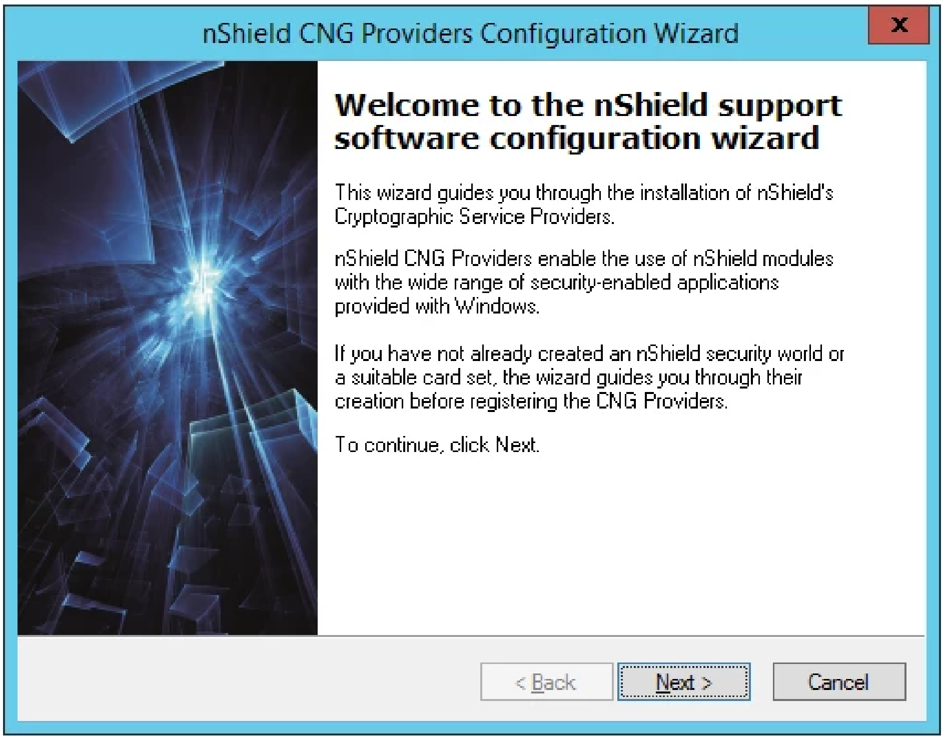
Configure KSP (Module protection)

NOTE: Please note that for the deployment of the Enterprise Gateway Server, you need to Configure KSP

1. In the Windows start up menu, run CNG wizard.



2. Click **Next**.



nShield CNG Providers Configuration Wizard

Welcome to the nShield support software configuration wizard

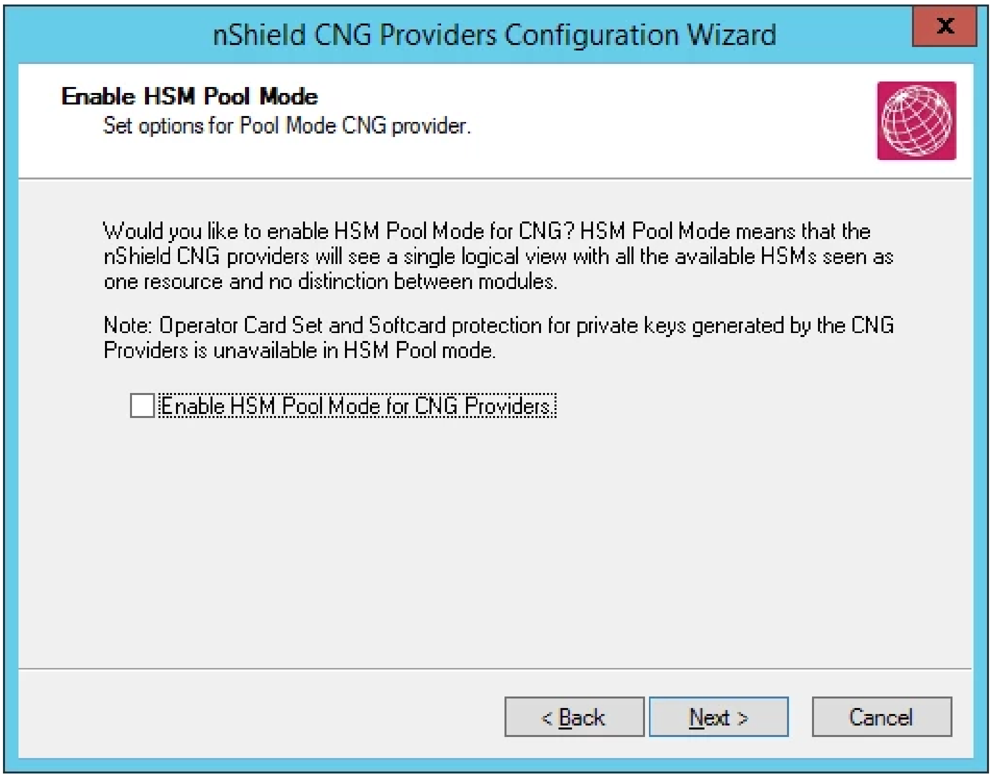
This wizard guides you through the installation of nShield's Cryptographic Service Providers.

nShield CNG Providers enable the use of nShield modules with the wide range of security-enabled applications provided with Windows.

If you have not already created an nShield security world or a suitable card set, the wizard guides you through their creation before registering the CNG Providers.

To continue, click Next.

3. On Enable HSM Pool Mode, click **Next.**



nShield CNG Providers Configuration Wizard

Enable HSM Pool Mode

Set options for Pool Mode CNG provider.

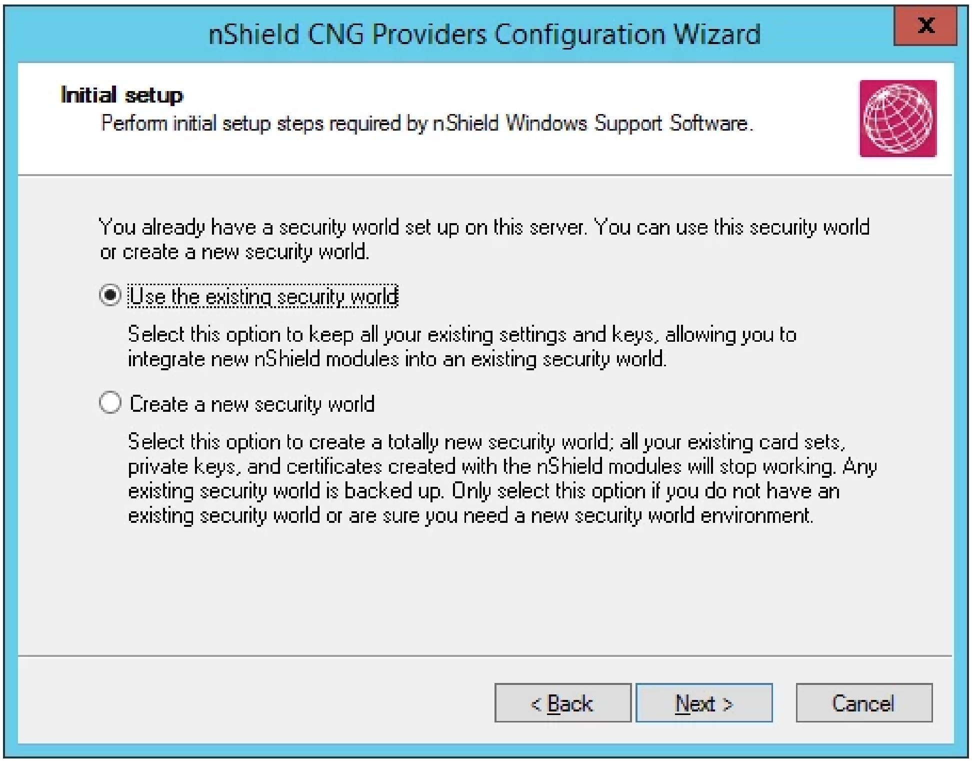
Would you like to enable HSM Pool Mode for CNG? HSM Pool Mode means that the nShield CNG providers will see a single logical view with all the available HSMs seen as one resource and no distinction between modules.

Note: Operator Card Set and Softcard protection for private keys generated by the CNG Providers is unavailable in HSM Pool mode.

☐ Enable HSM Pool Mode for CNG Providers

NOTE: Do not check the "Enable HSM Pool Mode for CNG Providers" checkbox.

4. On Initial setup dialog box, click **Next**.



Initial setup

Perform initial setup steps required by nShield Windows Support Software.

You already have a security world set up on this server. You can use this security world or create a new security world.

● Use the existing security world

Select this option to keep all your existing settings and keys, allowing you to integrate new nShield modules into an existing security world.

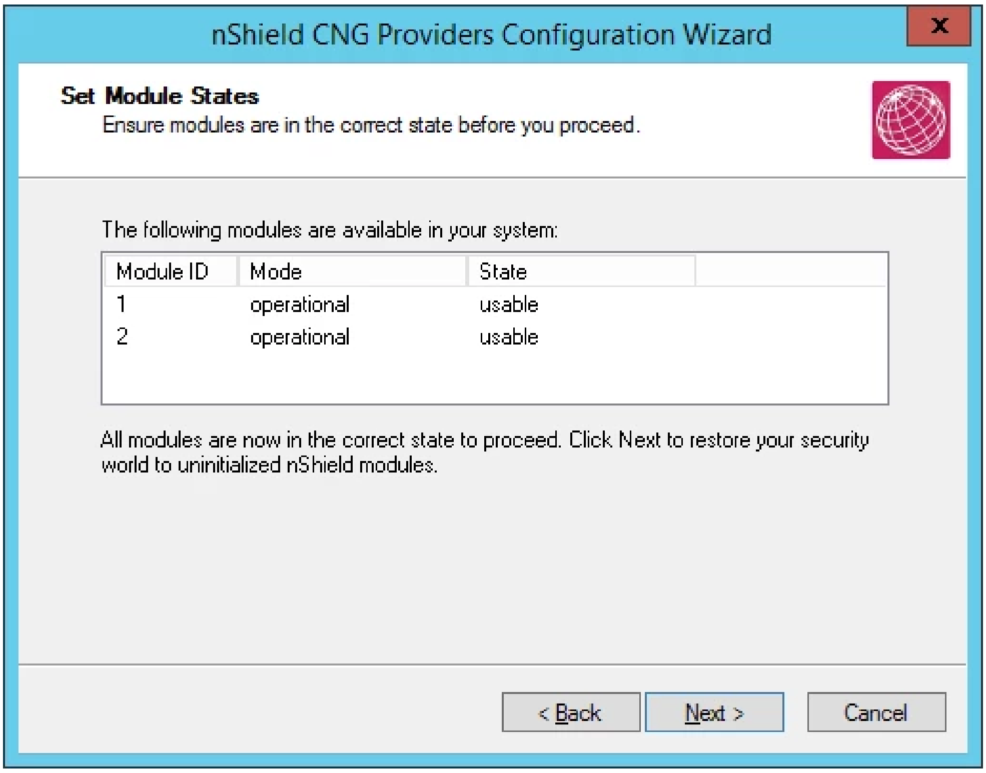
○ Create a new security world

Select this option to create a totally new security world; all your existing card sets, private keys, and certificates created with the nShield modules will stop working. Any existing security world is backed up. Only select this option if you do not have an existing security world or are sure you need a new security world environment.

NOTE: The first one (**Use the existing security world**) must be selectable. If not, please check the configuration of the module, for example rfs-sync.

---

5. On Module States dialog box, click **Next.**



Set Module States

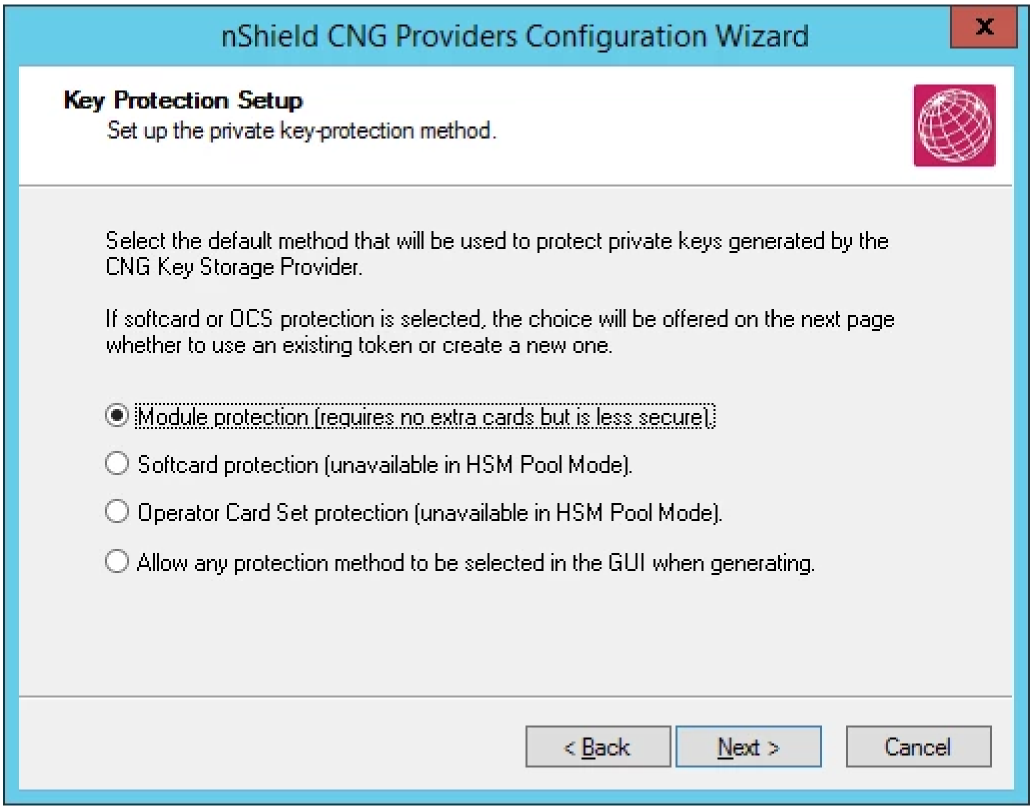
Ensure modules are in the correct state before you proceed.

The following modules are available in your system:

Module ID	Mode	State
1	operational	usable
2	operational	usable

All modules are now in the correct state to proceed. Click Next to restore your security world to uninitialized nShield modules.

6. On Key Protection Setup dialog box, click **Next**.



Key Protection Setup

Set up the private key-protection method.

Select the default method that will be used to protect private keys generated by the CNG Key Storage Provider.

If softcard or OCS protection is selected, the choice will be offered on the next page whether to use an existing token or create a new one.

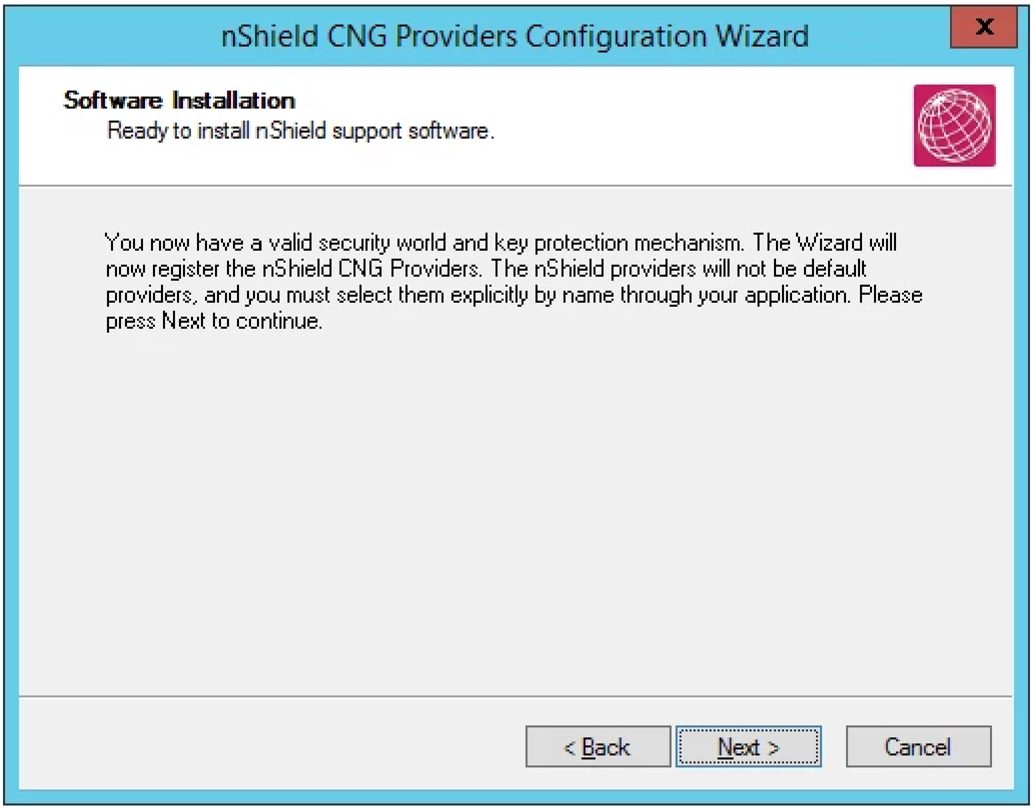
● Module protection (requires no extra cards but is less secure).

○ Softcard protection (unavailable in HSM Pool Mode).

○ Operator Card Set protection (unavailable in HSM Pool Mode).

○ Allow any protection method to be selected in the GUI when generating.

7. On Software Installation dialog box, click **Next.**

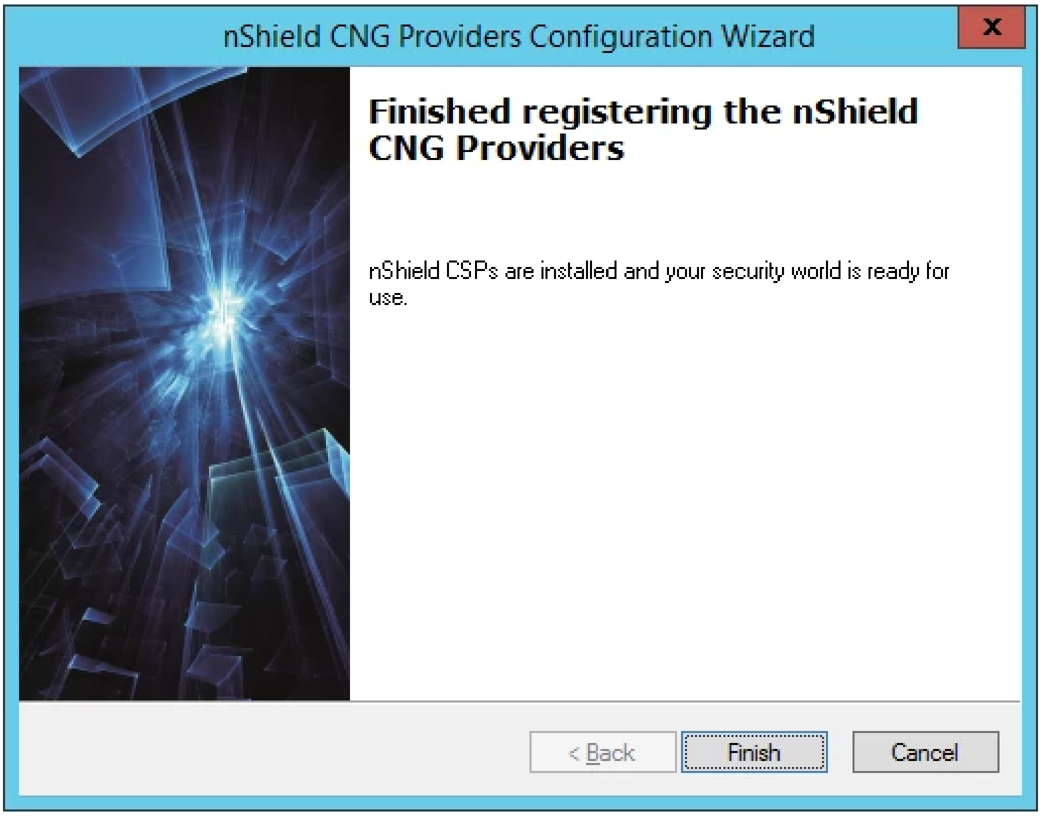


Software Installation

Ready to install nShield support software.

You now have a valid security world and key protection mechanism. The Wizard will now register the nShield CNG Providers. The nShield providers will not be default providers, and you must select them explicitly by name through your application. Please press Next to continue.

8. Click **Finish**.



nShield CNG Providers Configuration Wizard

Finished registering the nShield CNG Providers

nShield CSPs are installed and your security world is ready for use.

9. Confirm the providers for nCipher.

```
C:\Users\Administrator>cnglist --list-providers
Microsoft Key Protection 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
```

NOTE: You can find the following providers:

nCipher Primitive Provider
nCipher Security World Key Storage Provide

Generate CSR and Install Certificate (Module protection)

1. Create the information file for CSR.

   a) To generate CSR through certreq.exe through CSP, the ProviderName must be "nCipher Enhanced Cryptographic Provider". The sample of inf file follows:

```
[Version]
Signature = "$Windows NT$"
[NewRequest]
RequestType = PKCS10
ProviderName = "nCipher Enhanced Cryptographic Provider"
Subject = "CN=Registration Authority"
KeyContainer = "CSPRA20200316"
MachineKeySet = TRUE
KeyAlgorithm = RSA
KeyLength = 2048
KeyUsage = 0xf0
```

   b) To generate CSR through certreq.exe through KSP, the ProviderName must be "nCipher Security World Key Storage Provider". The sample of inf file is as follows:

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
RequestType = PKCS10
ProviderName = "nCipher Security World Key Storage Provider"
ProviderType = 0
Subject = "CN=Registration Authority"
KeyContainer = "KSPRA20190418"
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
```

2. Generate CSR through HSM.

NOTE: <inf-file> is the file created at step #1, <csr-file> is an output file.

   a) Open command prompt and run the following command:

```
> certreq -new <inf-file> <csr-file>
```

   b) The CSR file will be generated as follows:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDjzCCAncCAQAwITEfMB0GA1UEAwwWUmVnaXN0cmF0aW9uIEF1dGhvcml0eTCC
....
C610uaqncn6FvLu5pygZYFEVtOanCXNQRRUWiDGWKjHF+10GMh+V5YUur55T4W80
0uwK
-----END NEW CERTIFICATE REQUEST-----
```

3. Install a certificate.

    a) Open the command prompt (on the folder where the PKCS#7 file exists) and run the following command:

```
> certreq -accept <issued-cert>
```

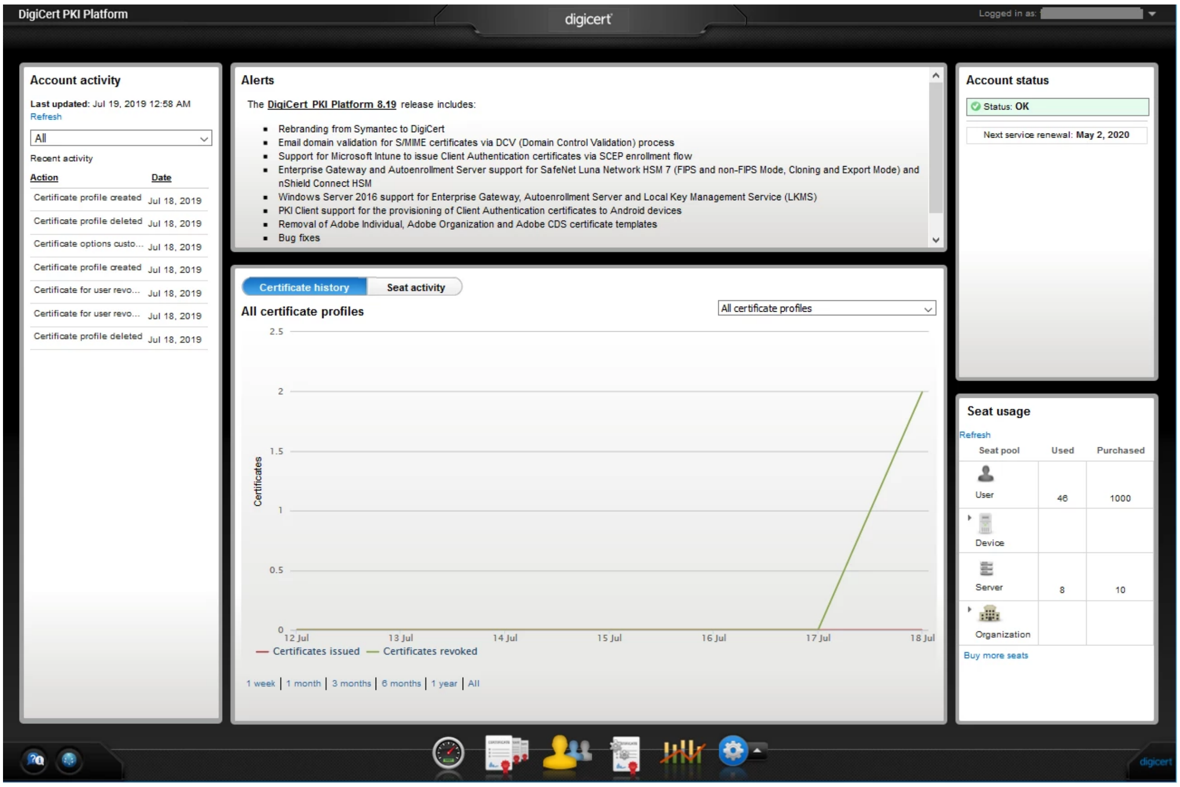
    b) Before running the command, the trusted root certificate must be installed. If not, the following error appears.

```
Certificate Request Processor: A certificate chain could not be built to a
trusted root authority. 0x800b010a (-2146762486 CERT_E_CHAINING)
```

Get RA Certificate in PKI-Manager

The generated CSR (PKCS#10) can be copied and pasted onto the "**Get an RA certificate**" page on PKI Manager by an authorized PKI Administrator. The resulting RA (PKCS#7) certificate can be saved onto a local folder.

1. Go to PKI Manager and use your certificate to sign in.



DigiCert PKI Platform

Logged in as: [redacted]

Account activity

Last updated: Jul 19, 2019 12:58 AM

Refresh

All

Recent activity

Action	Date
Certificate profile created	Jul 18, 2019
Certificate profile deleted	Jul 18, 2019
Certificate options custo...	Jul 18, 2019
Certificate profile created	Jul 18, 2019
Certificate for user revo...	Jul 18, 2019
Certificate for user revo...	Jul 18, 2019
Certificate profile deleted	Jul 18, 2019

Alerts

The DigiCert PKI Platform 8.19 release includes:

- Rebranding from Symantec to DigiCert
- Email domain validation for S/MIME certificates via DCV (Domain Control Validation) process
- Support for Microsoft Intune to issue Client Authentication certificates via SCEP enrollment flow
- Enterprise Gateway and Autoenrollment Server support for SafeNet Luna Network HSM 7 (FIPS and non-FIPS Mode, Cloning and Export Mode) and nShield Connect HSM
- Windows Server 2016 support for Enterprise Gateway, Autoenrollment Server and Local Key Management Service (LKMS)
- PKI Client support for the provisioning of Client Authentication certificates to Android devices
- Removal of Adobe Individual, Adobe Organization and Adobe CDS certificate templates
- Bug fixes

Account status

Status: OK

Next service renewal: **May 2, 2020**

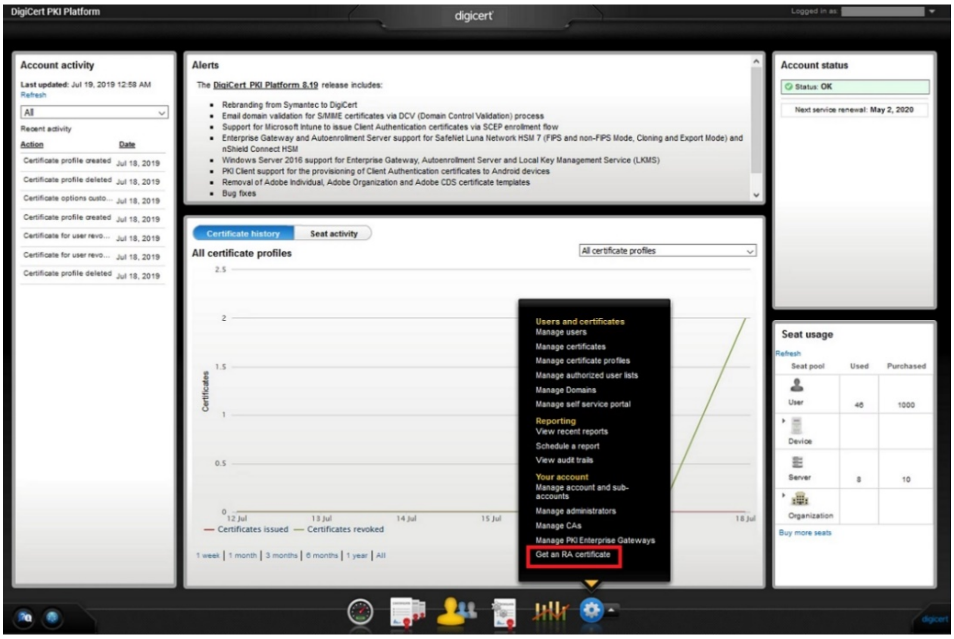
Seat usage

Refresh

Seat pool	Used	Purchased
User	46	1000
Device		
Server	8	10
Organization		

Buy more seats

2. Click Menu and select **Get an RA Certificate**.



Account activity

Last updated: Jul 19, 2019 12:58 AM

Refresh

All

Recent activity

Action	Date
Certificate profile created	Jul 18, 2019
Certificate profile deleted	Jul 18, 2019
Certificate options custo...	Jul 18, 2019
Certificate profile created	Jul 18, 2019
Certificate for user revo...	Jul 18, 2019
Certificate for user revo...	Jul 18, 2019
Certificate profile deleted	Jul 18, 2019

Alerts

The DigiCert PKI Platform 8.19 release includes:

- Rebranding from Symantec to DigiCert
- Email domain validation for S/MIME certificates via DCV (Domain Control Validation) process
- Support for Microsoft Intune to issue Client Authentication certificates via SCEP enrollment flow
- Enterprise Gateway and Autoenrollment Server support for SafeNet Luna Network HSM 7 (FIPS and non-FIPS Mode, Cloning and Export Mode) and nShield Connect HSM
- Windows Server 2016 support for Enterprise Gateway, Autoenrollment Server and Local Key Management Service (LKMS)
- PKI Client support for the provisioning of Client Authentication certificates to Android devices
- Removal of Adobe Individual, Adobe Organization and Adobe CDS certificate templates
- Bug fixes

Account status

Status: OK

Next service renewal: May 2, 2020

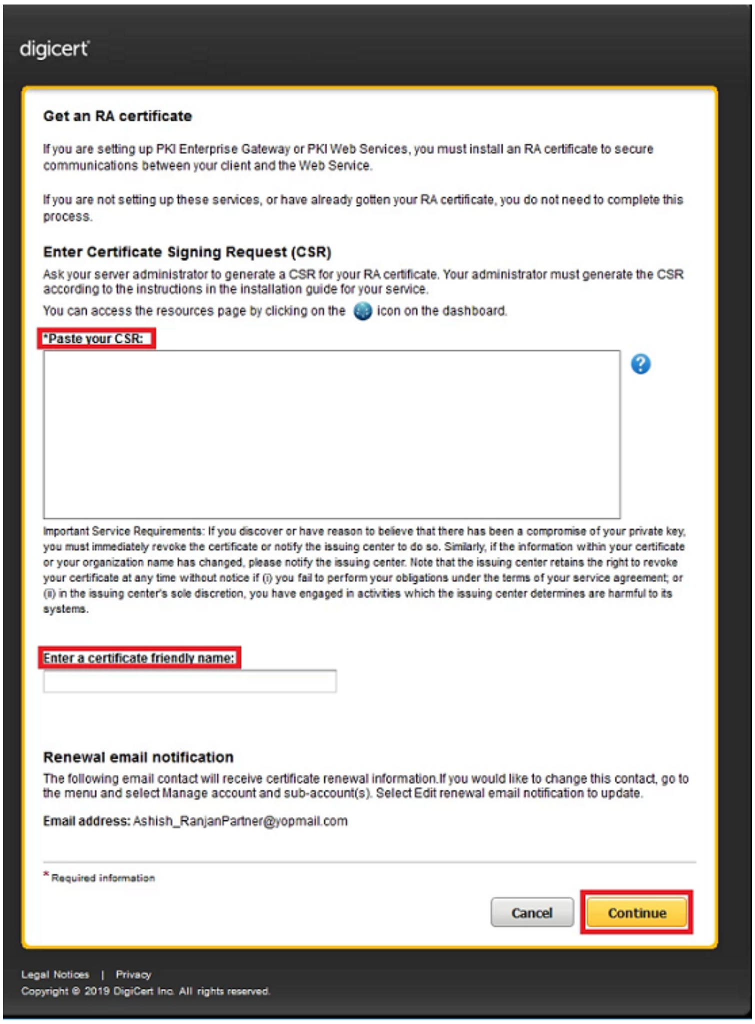
Seat usage

Refresh

Seat pool	Used	Purchased
User	46	1000
Device		
Server	8	10
Organization		

Buy more seats

3. Paste your CSR and enter a certificate friendly name and then click **Continue**.



Get an RA certificate

If you are setting up PKI Enterprise Gateway or PKI Web Services, you must install an RA certificate to secure communications between your client and the Web Service.

If you are not setting up these services, or have already gotten your RA certificate, you do not need to complete this process.

Enter Certificate Signing Request (CSR)

Ask your server administrator to generate a CSR for your RA certificate. Your administrator must generate the CSR according to the instructions in the installation guide for your service.

You can access the resources page by clicking on the 🌐 icon on the dashboard.

*Paste your CSR:

Important Service Requirements: If you discover or have reason to believe that there has been a compromise of your private key, you must immediately revoke the certificate or notify the issuing center to do so. Similarly, if the information within your certificate or your organization name has changed, please notify the issuing center. Note that the issuing center retains the right to revoke your certificate at any time without notice if (i) you fail to perform your obligations under the terms of your service agreement; or (ii) in the issuing center's sole discretion, you have engaged in activities which the issuing center determines are harmful to its systems.

Enter a certificate friendly name:

Renewal email notification

The following email contact will receive certificate renewal information.If you would like to change this contact, go to the menu and select Manage account and sub-account(s). Select Edit renewal email notification to update.

Email address: Ashish_RanjanPartner@yopmail.com

* Required information

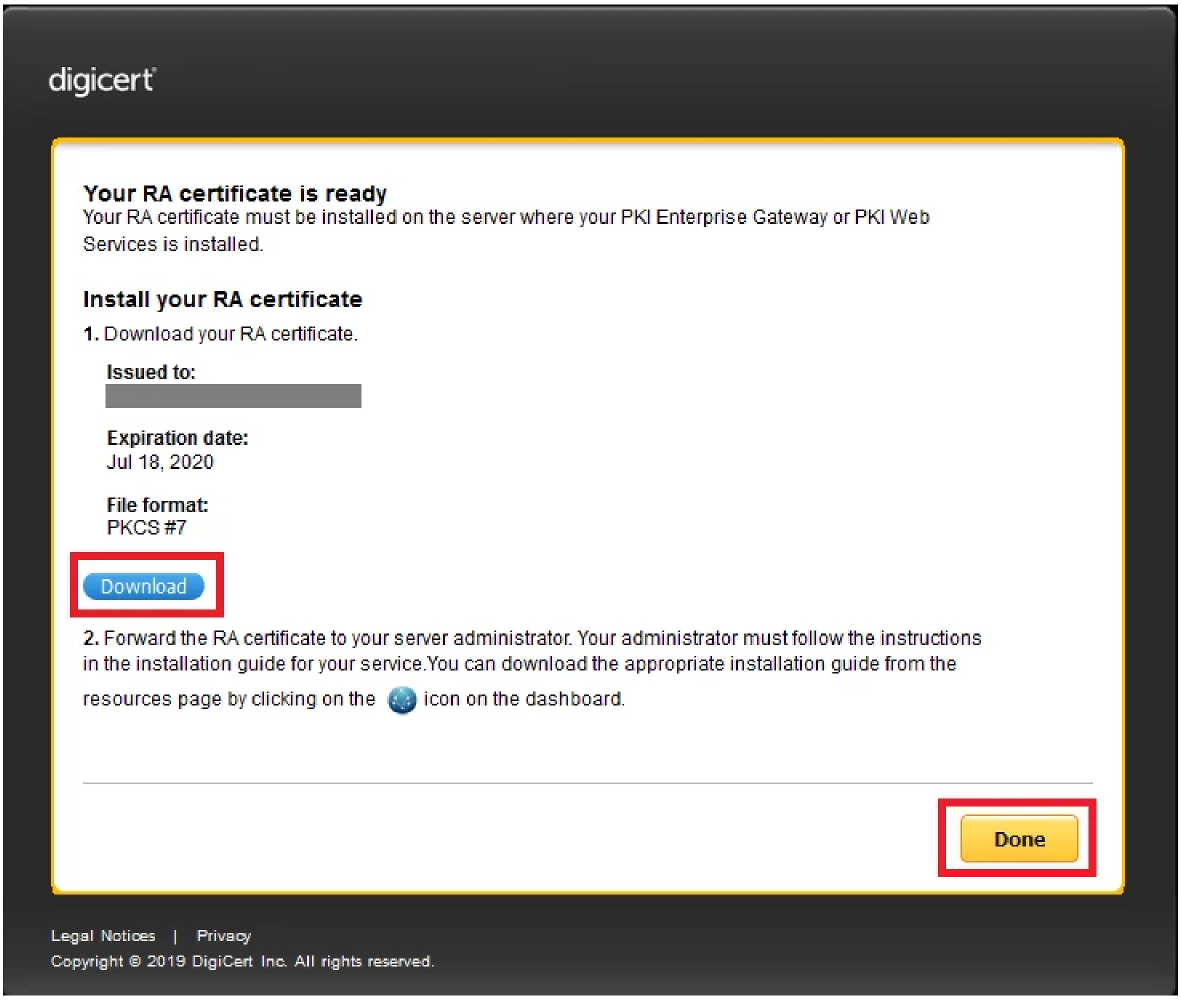
Legal Notices | Privacy

Copyright © 2019 DigiCert Inc. All rights reserved.

The CSR looks like the following. Paste it into the field.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDjzCCAncCAQAwITEfMB0GA1UEAwwWUmVnaXN0cmF0aW9uIEF1dGhvcml0eTCC
...
zbnTmg1IIY4NSgFcRsbs5j5GQDN86gSKmQ8/EvOjbpC62X3ZDhVmYSMBJUO1Jgv6
1tyz
-----END NEW CERTIFICATE REQUEST-----
```

4. Click **Download** to download the PKCS#7 file.



Your RA certificate is ready
Your RA certificate must be installed on the server where your PKI Enterprise Gateway or PKI Web Services is installed.

Install your RA certificate

1. Download your RA certificate.

Issued to:
[redacted]

Expiration date:
Jul 18, 2020

File format:
PKCS #7

2. Forward the RA certificate to your server administrator. Your administrator must follow the instructions in the installation guide for your service.You can download the appropriate installation guide from the resources page by clicking on the 🌐 icon on the dashboard.

Copyright © 2019 DigiCert Inc. All rights reserved.

5. Click **Done** to go back to the PKI Dashboard.