nShield Security World

nShield 5s v13.4.5 Install Guide

17 October 2024

Table of Contents

1. Introduction . . . 1
    1.1. About this guide . . . 1
    1.2. Model numbers . . . 1
    1.3. Terminology . . . 1
2. Hardware security modules . . . 2
    2.1. Electrical power requirements . . . 2
    2.2. Handling modules . . . 2
    2.3. Module operational temperature and humidity specifications . . . 2
    2.4. Cooling requirements . . . 3
        2.4.1. Cooling recommendations for a desktop installation . . . 4
        2.4.2. Cooling recommendations for a server installation . . . 4
    2.5. Physical location considerations . . . 4
3. Regulatory notices . . . 5
    3.1. FCC class A notice . . . 5
    3.2. Canadian certification - CAN ICES-3 (A)/NMB- 3(A) . . . 5
    3.3. Battery cautions . . . 5
    3.4. Hazardous substance caution . . . 5
    3.5. Recycling and disposal information . . . 5
4. Before installing the module . . . 6
    4.1. Back panel . . . 6
    4.2. Module pre-installation steps . . . 6
    4.3. Fitting a module bracket . . . 7
    4.4. User Replaceable items . . . 7
        4.4.1. Replace the battery . . . 8
5. Installing the module . . . 9
    5.1. Fitting a smart card reader . . . 9
    5.2. After installing the module . . . 9
6. Before you install the software . . . 11
    6.1. Preparatory tasks before installing software . . . 11
        6.1.1. Windows . . . 11
        6.1.2. Linux . . . 12
        6.1.3. All environments . . . 13
    6.2. Firewall settings . . . 15
7. Installing the software . . . 17
    7.1. Installing the Security World Software on Windows . . . 17
    7.2. Installing the Security World Software on Linux . . . 19
8. Setting the system clock . . . 22

8.1. Setting the HSM system clock . . . 22
9. Checking the installation . . . 23
9.1. Checking operational status . . . 23
9.1.1. Enquiry utility . . . 23
9.1.2. nFast server (hardserver) . . . 24
9.2. Log message types . . . 24
9.2.1. Information . . . 24
9.2.2. Notice . . . 25
9.2.3. Client . . . 25
9.2.4. Serious error . . . 25
9.2.5. Serious internal error . . . 25
9.2.6. Start-up errors . . . 25
9.2.7. Fatal errors . . . 26
10. HSM status and error codes . . . 27
10.1. LED status . . . 27
10.2. LED error states . . . 27
10.2.1. Error codes shown on the LED . . . 28
10.3. Error codes accessed remotely . . . 30
10.3.1. Runtime library errors . . . 30
10.3.2. Hardware driver errors . . . 30
10.3.3. Operational mode errors . . . 32
11. Uninstalling existing software . . . 33
11.1. Uninstalling the Security World Software on Windows . . . 34
11.2. Uninstalling the Security World Software on Linux . . . 34
12. Software packages on the Security World installation media . . . 36
12.1. Security World installation media . . . 36
12.1.1. Component bundles . . . 36
12.2. Components required for particular functionality . . . 37
12.2.1. KeySafe . . . 37
12.2.2. Microsoft CAPI CSP and Microsoft Cryptography API: Next Generation (CNG) . . . 38
12.3. nCipherKM JCA/JCE cryptographic service provider . . . 38
12.4. SNMP monitoring agent . . . 38

1. Introduction

The Entrust nShield 5s is a Hardware Security Module (HSM) for servers and appliances.

1.1. About this guide

This guide includes:

- Installing the nShield 5s. See Installing the module.
- Installing the Security World Software. See Installing the software.
- Steps to check the installation. See Checking the installation.
- A description of the module status indicators. See HSM status and error codes
- Instructions about removing existing software. See Uninstalling existing software.

See the *User Guide* for your module and operating system for more about, for example:

- Creating and managing a Security World
- Creating and using keys
- Card sets
- The advanced features of the nShield 5s.

For information on integrating Entrust nShield products with third-party enterprise applications, see https://www.entrust.com/digital-security/hsm.

1.2. Model numbers

Model numbering conventions are used to distinguish different nShield hardware security devices.

Model number	Used for
NC5536E-B	nShield 5s Base
NC5536E-M	nShield 5s Medium
NC5536E-H	nShield 5s High

1.3. Terminology

The nShield 5s is referred to as the nShield 5s, the *Hardware Security Module*, or the *HSM* in this guide.

2. Hardware security modules

2.1. Electrical power requirements

Module	Maximum power
nShield 5s	25W

Make sure that the power supply in your computer is rated to supply the required electric power.

The PCIe card, nShield 5s, is intended for installation into a certified personal computer, server, or similar equipment.

If your computer can supply the required electric power and sufficient cooling, you can install multiple modules in your computer.

2.2. Handling modules

The module contains solid-state devices that can withstand normal handling. However, do not drop the module or expose it to excessive vibration.

Before installing hardware, you must disconnect your computer from the power supply. Ensure that a grounded (earthed) contact remains. Perform the installation with care, and follow all safety instructions in this guide and from your computer manufacturer.

Static discharge can damage modules. Do not touch the module connec tor pins, or the exposed area of the module.

Leave the module in its anti-static bag until you are ready to install it. Always wear an anti-static wrist strap that is connected to a grounded metal object. You must also ensure that the computer frame is grounded while you are installing or removing an internal module.

2.3. Module operational temperature and humidity specifications

The nShield 5s module operates within the following environmental conditions.

nShield 5s environmental conditions	Operating range		Comments
	Min.	Max.	
Operating temperature*	5°C (41°F)	55°C (131°F)	Subject to sufficient airflow
Storage temperature	-5°C (-23°F)	60°C (140°F)	-
Transportation temperature	-40°C (-40°F)	70°C (158°F)	-
Operating humidity	5%	85%	Relative. Non-condensing at 30°C (86°F)
Storage humidity	5%	93%	Relative. Non-condensing at 30°C (86°F)
Transportation humidity	5%	93%	Relative. Non-condensing at 30°C (86°F)
Altitude	-100m (-328ft)	2000m (6561ft)	Above Mean Sea Level

*Air temperature at PCIe card inlet surface. For more information, see Cooling requirements.

The module is designed to operate in moderate climates only. Never operate the module in dusty, damp, or excessively hot conditions. Never install, store, or operate the module at locations where it may be subject to dripping or splashing liquids.

2.4. Cooling requirements

An air velocity of 1.9 m/s (373 LFM) is recommended for a module in operation.

During installation, ensure there is adequate airflow around the module. Airflow from fans must be directed to the inlet surface of the module such that air is flowing through and across the length of the module. To maximize airflow, use a PCIe slot with no neighboring modules if possible. If airflow is limited, consider fitting extra cooling fans.

The nShield 5s module is a passively cooled PCIe card that requires the host to provide sufficient airflow for cooling. Passive cards should not be powered without cooling airflow in place.

Ensure the module has adequate cooling. Failure to do so can result in damage to the module or computer.

To check the actual and maximum temperature of the module during operation, see the *Maintenance of nShield Hardware* section of the *User Guide* for your module and operating system. It is advised to do this directly after installing the module in its normal working environment. Monitor the temperature of the module over its first few days of operation.

2.4.1. Cooling recommendations for a desktop installation

For a desktop installation running in operating environmental conditions, dedicated airflow is required across the module. If the system cannot provide the necessary airflow, Entrust recommends you add a sufficiently powerful dedicated fan to directly cool the module. For details regarding the cooling requirements see Cooling requirements.

2.4.2. Cooling recommendations for a server installation

The desktop cooling recommendations further apply to a server installation. In addition, power and airflow control software is sometimes available in a server installation. If this is the case, Entrust recommends you:

- Configure the target air velocity in the software to ensure it does not fall below the airflow recommendations of the module. For details regarding the cooling requirements, see Cooling requirements.
- Ensure that the PCIe slot has been configured to fulfil the module power requirements.

2.5. Physical location considerations

For the certification of Entrust nShield HSM, refer to the *Security Manual*. In addition to the intrinsic protection provided by an nShield HSM, customers must exercise due diligence to ensure that the environment within which the nShield HSMs are deployed is configured properly and is regularly examined as part of a comprehensive risk mitigation program to assess both logical and physical threats. Applications running in the environment shall be authenticated to ensure their legitimacy and to thwart possible proliferation of malware that could infiltrate these as they access the HSMs' cryptographic services. The deployed environment must adopt 'defense in depth' measures and carefully consider the physical location to prevent detection of electromagnetic emanations that might otherwise inadvertently disclose cryptographic material.

3. Regulatory notices

3.1. FCC class A notice

The nShield 5s HSMs comply with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. The device may not cause harmful interference, and
2. The device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the users will be required to correct the interference at their own expense.

3.2. Canadian certification - CAN ICES-3 (A)/NMB- 3(A)

3.3. Battery cautions

Danger of explosion if the battery is incorrectly replaced. The battery may only be replaced with the same or equivalent type. Dispose of the used battery in accordance with your local disposal instructions.

3.4. Hazardous substance caution

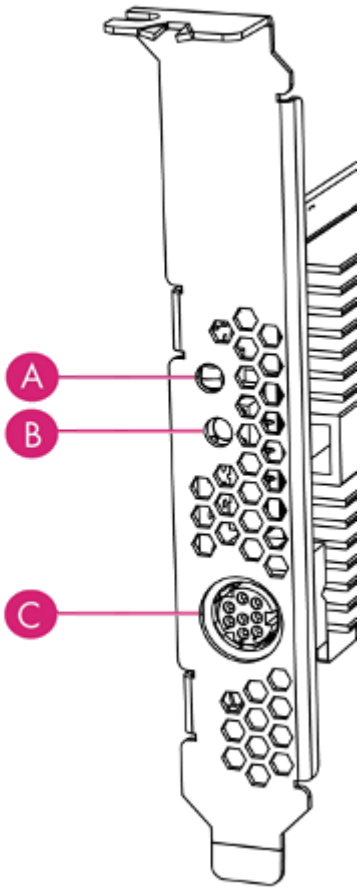
This product contains a lithium battery and other electronic components and materials which may contain hazardous substances. However, this product is not hazardous providing it is used in the manner in which it is intended to be used.

3.5. Recycling and disposal information

For recycling and disposal guidance, see the nShield product's *Warnings and Cautions* documentation.

4. Before installing the module

4.1. Back panel



Label	Description
A	Status LED
B	Recovery mode button
C	A mini-DIN connector for connecting a smart card reader.

4.2. Module pre-installation steps

Check the module to ensure that there is no sign of damage or tampering:

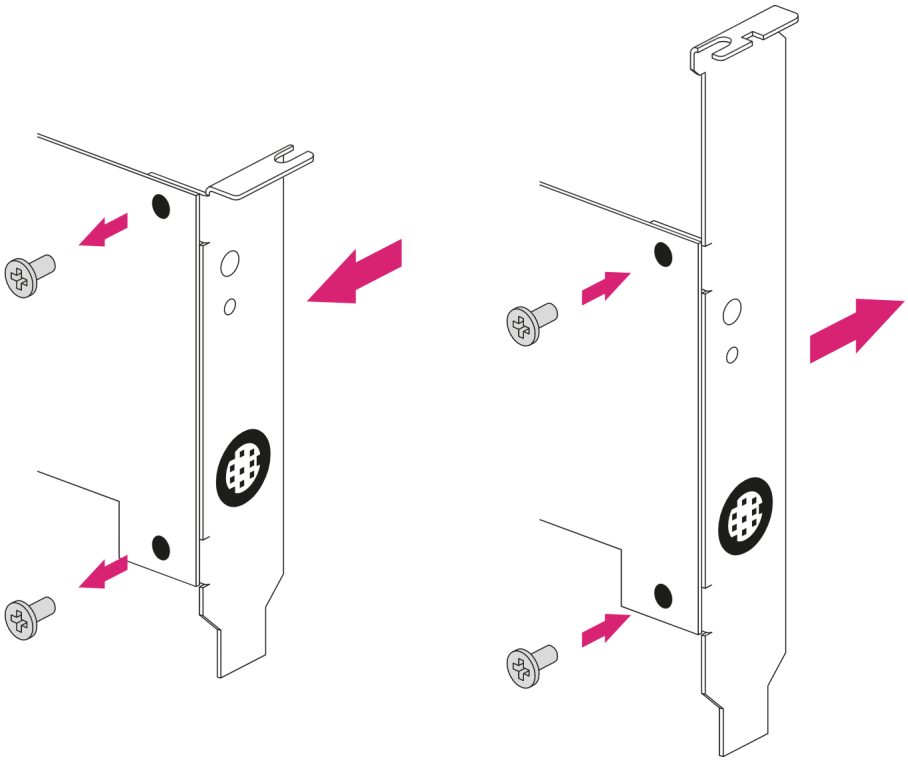
- Check the epoxy resin security coating for obvious signs of damage.
- If you intend to install the module with an external smart card reader, check the cable for signs of tampering. If evidence of tampering is present, do not use and request a

new cable.

4.3. Fitting a module bracket

Before installing a module in a PCI Express card slot, you may have to replace the bracket if it is not the same height as the slot. Both full height and low profile brackets are supplied with the module.

Do not touch the connector pins, or the exposed area of the module without taking electro-static discharge (ESD) precautions.



To fit the bracket to the module:

1. Remove the two screws from the solder side of the module.
2. Remove the incorrect bracket.
3. Fit the correct bracket to the component side of the module.
4. Insert the two screws into the solder side of the module to secure the bracket. Do not over tighten the screws.

4.4. User Replaceable items

If the module has been removed so that a part can be replaced, follow these procedures before installing the module. If no parts need replacing, proceed to Installing the module.

4.4.1. Replace the battery

Please follow battery disposal guidelines in the installation manual.

Required tools

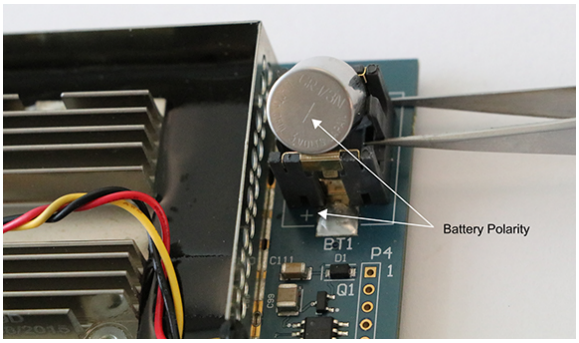
- Small non-conductive tweezers

Required part

- Orderable part number: SOLOXC-REP-BATT (Replacement battery)

To remove and replace the battery:

1. Power off the system and while taking ESD precautions, remove the module.
2. Place the module on a flat surface.
3. Using the tweezers, gently remove the battery from the BT1 connector.



4. Observing the polarity, install the replacement battery in the BT1 connector.
5. Re-install the module into the PCIe slot.

5. Installing the module

1. Power off the system and while taking electrostatic discharge precautions, remove the module from its packaging.
2. Open the computer case and locate an empty PCIe slot. If necessary, follow the instructions that your computer manufacturer supplied.

   You must only install your nShield 5s module into a PCIe slot. See the instructions that your computer manufacturer supplied to correctly identify the slots on your computer.

   Minimum requirement: 1 PCIe x4 slot
3. If there is a blanking plate across the opening to the outside of the computer, remove it. Check that the opening is large enough to enable you to access the module back panel.
4. Insert the contact edge of the module into the empty slot. Press the card firmly into the connector to ensure that:
   - The contacts are fully inserted in the connector
   - The back panel is correctly aligned with the access slot in the chassis
5. Use the bracket screw or fixing clip to secure the module to the computer chassis.
6. Replace the computer case.

5.1. Fitting a smart card reader

Connect the smart card reader to the connector on the back panel of the module. A D-type to mini-DIN adapter cable is supplied with the module.

5.2. After installing the module

If the Security World software has not already been installed, you must install the Security World Software by following the instructions at Installing the software.

Although methods of installation vary from platform to platform, the Security World Software should automatically detect the module on your computer and install the drivers. You do not have to restart the system.

If this is not the first HSM installed in this host, the Security World software is already installed and you can skip the instructions at Installing the software. However, you still need to set up communication between the host and the newly installed module. The module

must either be in factory state or have been previously prepared for use on this host. For more information, see *Set up communication between host and module* in the *User Guide* for your module and operating system.

If the new module has been supplied from the factory it will already be in factory state.

6. Before you install the software

Before you install the software, you should:

- Install the module. See Installing the module.
- Uninstall any older versions of Security World Software. See Uninstalling existing software.
- If the nShield Remote Administration Client is installed on the machine, remove it. You will also have to re-install it after you installed the new Security World software version. See the *nShield Remote Administration User Guide*.
- Complete any other necessary preparatory tasks, as described in Preparatory tasks before installing software.

6.1. Preparatory tasks before installing software

Perform any of the necessary preparatory tasks described in this section before installing the Security World Software.

6.1.1. Windows

6.1.1.1. Power saving options

Adjust your computers power saving setting to prevent sleep mode.

You may also need to set power management properties of the HSM, once the Security World Software is installed. See Installing the Security World Software on Windows for more information.

6.1.1.2. Install Microsoft security updates

Make sure that you have installed the latest Microsoft security updates. Information about Microsoft security updates is available from http://www.microsoft.com/security/.

6.1.1.3. Add %NFAST_HOME%\bin\ to the PATH environment variable

The default location for `%NFAST_HOME%\bin\` is `C:\Program Files\nCipher\nfast`. Because of the space in `Program Files`, nShield commands could fail if `NFAST_HOME\bin\` is not in `PATH`.

If you cannot change `PATH`, you will have to enclose all file names and paths that use vari-

able between double quotation marks (" "). For example:

```
"%NFAST_HOME%\toolkits\pkcs11\cknfast.dll"
```

6.1.2. Linux

6.1.2.1. Install operating environment patches

Make sure that you have installed:

- kernel packages like `gcc`, `kernel-headers`, `kernel-devel`
- the latest recommended patches for your environment in general

See the documentation supplied with your operating environment for information.

6.1.2.2. Users and groups

The installer automatically creates the following group and users if they do not exist. If you wish to create them manually, you should do so before running the installer. Create the following, as required:

- The `nfast` user in the `nfast` group, using `/opt/nfast` as the home directory.
- If you are installing SNMP, the `ncsnmpd` user in the `ncsnmpd` group, using `/opt/nfast` as the home directory.
- If you are installing the Remote Administration Service, the `raserv` user in the `raserv` group, using `/opt/nfast` as the home directory.

6.1.2.3. Network configuration

The nShield 5s appears to the host operating system as a network interface. Communication with the HSM is performed over this interface using IPv6. The install process automatically configures the nShield 5s and any relevant operating system network settings, with the HSM and host-software using link-local communication.

After the installation process has been completed, the nShield 5s network interfaces should have a link-local IPv6 address. On Windows and Linux, this is assigned automatically. On Linux, the installation process will also detect the following network management services and create appropriate configuration files:

Network management service	Configuration file path
`NetworkManager`	`/etc/network/interfaces.d/nshield`
`systemd.networkd`	`/etc/systemd/network/nshield.network`

These files instruct the network management service not to configure the nShield 5s interfaces. They will be configured by the nShield host software. This covers all of our supported distributions, and more. If your distribution is not using one of these network management services, you will need to configure the interfaces to have a link-local IPv6 address manually.

The following network configuration must be present for the host software and HSM to function:

- The HSM's network interface must be assigned a link-local IPv6 address (https://tools.ietf.org/html/rfc4862).
- Multicast DNS must be possible for the host software to discover the services running on the HSM (https://tools.ietf.org/html/rfc6762).

  This requires inbound UDP packets on port 5353, to receive service advertisement responses from the HSM.

- The following ports must be accessible on the HSM from the host to access management and crypto services.

  Outbound SSH traffic on TCP ports:

  - 2201
  - 2202
  - 2203
  - 2204
  - 2206

6.1.3. All environments

6.1.3.1. Install Java with any necessary patches

The following versions of Java have been tested to work with, and are supported by, your nShield Security World Software:

- Java7 (or Java 1.7x)

- Java8 (or Java 1.8x)
- Java11.

Entrust recommends that you ensure Java is installed before you install the Security World Software. The Java executable must be on your system path.

If you can do so, please use the latest Java version currently supported by Entrust that is compatible with your requirements. Java versions before those shown are no longer supported. If you are maintaining older Java versions for legacy reasons, and need compatibility with current nShield software, please contact Entrust nShield Support, https://nshieldsupport.entrust.com.

To install Java, you may need installation packages specific to your operating system, which may depend on other pre-installed packages to be able to work.

Suggested links from which you may download Java software as appropriate for your operating system:

- http://www.oracle.com/technetwork/java/index.html
- http://www.oracle.com/technetwork/java/all-142825.html

You must have Java installed to use KeySafe.

6.1.3.2. Identify software components to be installed

Entrust supply standard component bundles that contain many of the necessary components for your installation and, in addition, individual components for use with supported applications. To be sure that all component dependencies are satisfied, you can install either:

- All the software components supplied
- Only the software components you require

During the installation process, you are asked to choose which bundles and components to install. Your choice depends on a number of considerations, including:

- The types of application that are to use the module
- The amount of disc space available for the installation
- Your company's policy on installing software. For example, although it may be simpler to choose all software components, your company may have a policy of not installing any software that is not required.

On Windows, the **nShield Hardware Support bundle** and the **nShield Core Tools bundle** are

mandatory, and are always installed.

On Windows, the **Windows device drivers** component is installed as part of the **Hardware Support bundle**. On Linux, the **Kernel device drivers** component is installed.

On Linux, you *must* install the `hwsp` component and the `nshield5_net` component.

The **Core Tools bundle** contains all the Security World Software command-line utilities, including:

- `generatekey`
- Low level utilities
- Test programs

The Core Tools bundle includes the **Tcl run time** component that installs a run-time Tcl installation within the nCipher directories. This is used by the tools for creating the Security World and by KeySafe. This does not affect any other installation of Tcl on your computer.

You need to install the Remote Administration Service component if you require remote administration functionality. See Preparatory tasks before installing software and the *User Guide* for your module and operating system for more about the Remote Administration Service.

Always install all the nShield components you need in a single installation process to avoid subsequent issues should you wish to uninstall. You should not, for example, install the Remote Administration Service from the Security World installation media, then later install the Remote Administration Client from the client installation media.

Ensure that you have identified any optional components that you require before you install the Security World Software. See Software packages on the Security World installation media for more about optional components.

6.2. Firewall settings

When setting up your firewall, you should ensure that the port settings are compatible with the HSMs and allow access to the system components you are using. The following table identifies the ports used by the nShield system components. All listed ports are the default setting. Other ports may be defined during system configuration, according to the requirements of your organization.

Component	Default Port	Protocol	Use
Hardserver	9000	TCP	Internal non-privileged connections from Java applications including KeySafe
Hardserver	9001	TCP	Internal privileged connections from Java appli cations including KeySafe
Hardserver	9004	TCP	Incoming impath connections from other hard servers, for example: * From a cooperating client to the remote file system it is configured to access * From a non-attended host machine to an attended host machine when using Remote Operator
Remote Administration Ser-vice	9005	TCP	Incoming connections from Remote Adminis-tration Clients
Audit Logging syslog	514	UDP	If you plan to use the Audit Logging facility with remote syslog or SIEM applications, you need to allow outgoing connections to the configured UDP port
mDNS	5353	UDP	Send out mDNS Service Discovery requests and receive responses

If you are using an nShield Edge as a Remote Operator slot for an HSM located elsewhere, you need to open port 9004. You may restrict the IP addresses to those you expect to use this port. You can also restrict the IP addresses accepted by the hardserver in the configura tion file. See the *User Guide* for your module and operating system for more about configu-ration files. Similarly, if you are setting up the Remote Administration Service you need to open port 9005.

7. Installing the software

This chapter describes how to install the Security World Software on the host computer.

After you have installed the software, you must complete further Security World creation, configuration and setup tasks before you can use your nShield environment to protect and manage your keys. See the *User Guide* for your module and operating system for more about creating a Security World and the appropriate card sets, and further configuration or setup tasks.

7.1. Installing the Security World Software on Windows

For information about configuring silent installations and uninstallations on Windows, see the *User Guide*.

For a regular installation:

Installing Security World software on Windows via Remote Desktop Connection can result in a brief loss of RDP connection. If this happens, it will happen during the **Status:** part of the installation, towards the end. When the session reconnects, the installation carries on until completion.

1. Sign in as an Administrator or as a user with local administrator rights.

   If the Found New Hardware Wizard appears and prompts you to install drivers, cancel this notification, and continue to install the Security World Software as normal. Drivers are installed during the installation of the Security World Software.

2. Place the Security World Software installation media in the optical disc drive.
3. Launch `setup.msi` manually when prompted.
4. Follow the onscreen instructions.
5. Accept the license terms and select **Next** to continue.
6. Specify the installation directory and select **Next** to continue.
7. Select all the components required for installation.

   By default, all components are selected. Use the drop-down menu to deselect the components that you do not want to install. **nShield Hardware Support** and **Core Tools** are necessary to install the Security World Software.

See Software packages on the Security World installation media for more about the component bundles and the additional software supplied on your installation media.

8. Select **Install**.

   The selected components are installed in the installation directory chosen above. The installer creates links to the following nShield Cryptographic Service Provider (CSP) setup wizards as well as remote management tools under **Start** > **Entrust** or **Entrust nShield Security World** (depending on the version of Windows or Windows Server you are running):

   - If **nShield CSPs (CAPI, CNG)** was selected: **32bit CSP install wizard**, which sets up CSPs for 32-bit applications
   - If **nShield CSPs (CAPI, CNG)** was selected: **64bit CSP install wizard**, which sets up CSPs for 64-bit applications
   - If **nShield CSPs (CAPI, CNG)** was selected: **CNG configuration wizard**, which sets up the CNG providers
   - If **nShield Java** was selected: **KeySafe**, which runs the key management application
   - If **nShield Remote Administration Client Tools** was selected: **Remote Administration Client**, which runs the remote administration client

   If selected, the SNMP agent will be installed, but will not be added to the **Services** area in **Control Panel** > **Administrative Tools** of the target Windows machine. If you wish to install the SNMP agent as a service, please consult the *SNMP monitoring agent* section in the *User Guide* for your module and operating system.

   Do not run any CSP installation wizard before installing the module hardware.

9. Select **Finish** to complete the installation.

   The following global variables are set upon install:

   - `%NFAST_CERTDIR%`
   - `%NFAST_HOME%`
   - `%NFAST_KMDATA%`
   - `%NFAST_LOGDIR%`
   - `%NFAST_SERVICES_HOME%`

10. Stop the nFast Server service.
11. The nShield installer creates and enables an inbound rule called `nShield 5s mDNS` to

allow UDP port 5353 for any program. This enables the discovery of nShield 5s modules. If enrollment fails to find any modules in the following step, check that this firewall rule is present and enabled; if it does not exist, create it manually and retry enrollment.

12. Set up the secure communication channels between the host PC and the HSM:

```
"%NFAST_HOME%\bin\hsmadmin" enroll
```

The HSM must be in factory state or else the registered `sshadmin` key must be in place otherwise this command will fail. If you have a backup of your `sshadmin` key, you can restore it using `hsmadmin keys restore`. If this is not a first-time installation of this HSM, and the `sshadmin` key trusted by this HSM is no longer available, enter recovery mode and then retry enrollment.

13. Start the nFast Server service.
14. If Remote Administration is installed, also start the nFast Remote Administration service.
15. Entrust recommends that you take a backup of your `sshadmin` key with `hsmadmin keys backup path\to\backup_key` for backups that will be restored to the same machine. Note that this key will not be usable on another machine or if the OS is re-installed as it has protections tied to the local machine. For backups that may be restored to a different machine or re-installed OS, use `hsmadmin keys backup --passphrase path\to\backup_key` to protect the key with a user-supplied passphrase. Replace `path\to\backup_key` with the actual path to where the backup key should be written in the example commands above.

You may additionally need to do the following after you have installed the software:

- In **Windows Device Manager** > **Network adapters**, select the appropriate module.
- Under **Properties > Power Management**, deselect **Allow the computer to turn off this device to save power**.

7.2. Installing the Security World Software on Linux

In the following instructions, *disc-name* is the name of the mount point of the installation media.

1. Sign in as a user with root privileges.
2. Mount the DVD/ISO image.

3. Open a terminal window, and change to the root directory.
4. Extract the required `.tar.gz` files to install all the software bundles by running commands of the form:

   ```
   sudo mkdir /opt/nfast
   sudo tar zxf /<iso-mountpoint>/linux/amd64/<file>.tar.gz -C /opt/nfast/
   ```

   In this command, `<file>` is the name of a `.tar.gz` file for that component, for example `hwsp.tar.gz`.

   See Software packages on the Security World installation media for more about the component bundles and the additional software supplied on your installation media.

5. To use an nShield module with your Linux system, you must build a kernel driver. Entrust supplies the source to the NFP and a makefile for building the driver as a loadable module.

   The kernel level driver is installed as part of the `hwsp` bundle. To build the driver with the supplied makefile, you must have the correct headers installed for the kernel that you are running. They must be headers for the same version of the kernel and must contain the kernel configuration options with which your kernel was built. You must also have appropriate versions of `gcc`, `make`, and your C library's development package.

   The configuration script looks for the kernel headers in the default directory `/lib/modules/'<uname -r>'/build/include/`. If your kernel headers are located in a different directory, set the `KERNEL_HEADERS` environment variable so that they are in `$KERNEL_HEADERS/include/`. Historically, the headers have resided in `/usr/src/linux/include/`. If the headers for your kernel are not already installed, install them from your Linux distribution disc, or contact your kernel supplier.

   Build the driver as a loadable kernel module. When you have ensured the correct headers are in place, perform the following steps to use the makefile:

   a. Change directory to the nShield PCI driver directory by running the command:

      ```
      # cd /opt/nfast/driver-nshield5
      ```

   b. Make the driver by running the command:

      ```
      # make
      ```

      This produces a driver file that is automatically loaded as part of the normal installation process.

6. Run the install script by using the following command:

```
/opt/nfast/sbin/install
```

7. Sign in to your normal account.
8. Add `/opt/nfast/bin` to your `PATH` system variable:

   If you use the Bourne shell, add these lines to your system or personal profile:

```
PATH=/opt/nfast/bin:$PATH
export PATH
```

   If you use the C shell, add this line to your system or personal profile:

```
setenv PATH /opt/nfast/bin:$PATH
```

9. Entrust recommends that you take a backup of your `sshadmin` key. For example, you could use `hsmadmin keys backup /root/.ssh/id_nshield5_sshadmin` for backups that will be restored to the same machine. If the path `/root/.ssh/id_nshield5_sshadmin` is used, and the `sshadmin` key is missing from the usual installed location under `/opt/nfast`, then that key will be used automatically when running the nShield install script. Note that this key will not be usable on another machine or if the OS is re-installed as it has protections tied to the local machine. For backups that may be restored to a different machine or re-installed OS, use `hsmadmin keys backup --passphrase /path/to/backup_key` to protect the key with a user-supplied passphrase (replacing `/path/to/backup_key` with the actual path to where the backup key should be written).

8. Setting the system clock

Entrust recommends that you set the HSM system clock before performing any other actions. This is because the HSM clock may have drifted from real time whilst the HSM was running on battery power in storage.

The HSM system clock is set by fetching the current time and date from the host machine in which the HSM is fitted. Therefore it is important to check that the time and date is set correctly on the host machine.

Initial setting of the HSM system clock should be performed with the HSM in maintenance mode. If your HSM is not in maintenance, you must put it into maintenance mode. For instructions, see the *User Guide* for your HSM.

8.1. Setting the HSM system clock

1. Make sure that the date and time on the host machine are set correctly according to the documentation for the operating system on the host machine.
2. Run the following command as a user with `root` privileges on Linux or the privileges of the built-in local Administrators group on Windows:

```
/opt/nfast/bin/hsmadmin settime
```

When you are setting time at the very first time on an nShield 5s HSM, it is recommended to avoid the optional `--adjust` parameter. This parameter is intended to be used when the HSM is already in operational mode. It can be used on a periodic basis to gradually reconcile any discrepancies between the host's and the HSM's clocks. Gradual reconciliation prevents sudden time discrepancies and ensures smooth operation.

9. Checking the installation

This section describes what to do if you have an issue with the module or the software.

The facilities described below are only available if the software has been installed successfully.

9.1. Checking operational status

9.1.1. Enquiry utility

Run the `enquiry` utility to check that the module is working correctly. You can find the `enquiry` utility in the `bin` subdirectory of the `nCipher` directory. This is usually:

- `C:\Program Files\nCipher\nfast` for Windows
- `/opt/nfast` for Linux

If the module is working correctly, the `enquiry` utility returns a message similar to the follow ing:

```
Server:
enquiry reply flags  none
enquiry reply level  Six
serial number        #############-####
mode                 operational
version              #.#.#
speed index          ###
rec. queue           ##..##
...
module type code     0
product name         nFast server
...
Module ##:
enquiry reply flags  none
enquiry reply level  Six
serial number        #############-####
mode                 operational
version              #.#.#
speed index          ###
rec. queue           ##..##
...
module type code     14
product name         #######/#######
...
rec. LongJobs queue  ##
SEE machine type     None
supported KML types  DSAp1024s160 DSAp3072s256
active modes         none
physical serial      48-U50104
hardware part no     PCA10005-01 revision 03
hardware status      OK
```

If the mode is operational the module has been installed correctly.

If the mode is initialization or maintenance, the module has been installed correctly, but you must change the mode to operational. See the *User Guide* for your module and operating system for more about changing the module mode.

If the output from the `enquiry` command says that the module is not found, first restart your computer, then re-run the `enquiry` command.

If the operating system supports power saving, disable power saving. See Installing the module for more information. Otherwise, if your system enters Sleep mode, the HSM may not be found when running `enquiry`. If this happens, you need to reboot your system.

9.1.2. nFast server (hardserver)

Communication can only be established with a module if the nFast server is running. If the server is not running, the `enquiry` utility returns the message:

```
NFast_App_Connect failed: ServerNotRunning
```

Restart the nFast server, and run the `enquiry` utility again. See the *User Guide* for your module and operating system for more about how to restart the nFast server.

9.2. Log message types

By default, the hardserver writes log messages to:

- The in Windows Operating System event log.
- `log/logfile` in the `nCipher` directory (normally `opt/nfast/log` directory) on Linux. The environment variable `NFAST_SERVERLOGLEVEL` determines what types of message you see in your log. The default is to display all types of message. For more information on `NFAST_SERVERLOGLEVEL`, see the *User Guide* for your module and operating system.

`NFAST_SERVERLOGLEVEL` is a legacy debug variable.

9.2.1. Information

This type of message indicates routine events:

```
nFast Server service: about to start
nFast Server service version starting
```

```
nFast server: Information: New client clientid connected
nFast server: Information: New client clientid connected - privileged
nFast server: Information: Client clientid disconnected
nFast Server service stopping
```

9.2.2. Notice

This type of message is sent for information only:

```
nFast server: Notice: message
```

9.2.3. Client

This type of message indicates that the server has detected an error in the data sent by the client (but other clients are unaffected):

```
nFast server: Detected error in client behaviour: message
```

9.2.4. Serious error

This type of message indicates a serious error, such as a communications or memory failure:

```
nFast server: Serious error, trying to continue: message
```

If you receive a serious error, even if you are able to recover, contact Support.

9.2.5. Serious internal error

This type of message indicates that the server has detected a serious error in the reply from the module. These messages indicate a failure of either the module or the server:

```
nFast server: Serious internal error, trying to continue: message
```

If you receive a serious internal error, contact Support.

9.2.6. Start-up errors

This type of message indicates that the server was unable to start:

```
nFast server: Fatal error during startup: message nFast Server service version failed init.
```

```
nFast Server service version failed to read registry
```

Reinstall the server as described in the *User Guide* for your module and operating system. If this does not solve the problem, contact Support.

9.2.7. Fatal errors

This type of message indicates a fatal error for which no further reporting is available:

```
nFast server: Fatal internal error
```

or

```
nFast server: Fatal runtime error
```

If you receive either of these errors, contact Support.

10. HSM status and error codes

The Entrust nShield 5s HSM is fitted with a tri-color LED on the back panel. This LED will typically indicate the operational state of the HSM, see LED status. However, the LED can also indicate if the HSM is in an unrecoverable error state, see LED error states. Unrecoverable error state codes can also be retrieved remotely using the `enquiry` utility, see Error codes accessed remotely.

10.1. LED status

The Entrust nShield 5s HSM is fitted with a tri-color LED on the back panel. This LED typically indicates the status of the HSM.

The following states indicate a normal operational state:

Colour	Pattern	Meaning
N/A	Blank	No power or processors not working.
Green	Solid	Power is good. Main processor has not started booting.
Cyan	Solid	Main processor is booting.
Cyan/Blue	Slow flash	Security processor firmware upgrade in progress.
Blue	Solid	System has booted, now idle.
Blue	Flickering	System is active - normal operation.

The following states indicate an error within the HSM:

Colour	Pattern	Meaning
Blue	Morse code	Error state for when the HSM is in an unrecoverable state, see LED error states for more information.
Red	Morse code	Error state for when the HSM is in an unrecoverable state see LED error states for more information.
Red	Fast flash	Security processor bootloader failure.
Blue/Red	Flash	Security processor detected a tamper condition.
Other	Any	Contact Entrust Support.

10.2. LED error states

If the Entrust nShield 5s HSM encounters an unrecoverable error, it enters an error state. In an error state, the HSM does not respond to commands and does not write data to the bus. The LED displays a Morse code pattern to indicate a specific error state, see Error codes shown on the LED.

In some cases you can reset an HSM in an error state by powering down the HSM and then reapplying power, or with `hsmadmin reset`. Not all errors can be reset in this way.

If any HSM goes into an error state, except as a result of you issuing the `nopclearfail --fail` command, contact Entrust Support, and give full details of your HSM set-up and the error code.

Entrust recommends that you contact Entrust Support even if you successfully recover from the error.

For troubleshooting information, see the relevant *Installation Guide* for your HSM.

10.2.1. Error codes shown on the LED

If an HSM enters an error state, the LED flashes with a Morse code pattern corresponding to an error code.

Error codes can also be retrieved remotely using the `enquiry` utility, see Error codes accessed remotely.

All the LED error codes have three digits:

- The first digit is indicated by a number of dots.
- The second digit is then indicated by a number of dashes.
- The third digit is then indicated by a number of dots.

There is then a longer gap and the error code repeats.

The following guidelines are useful when reading LED code messages from the HSM:

- The duration of a dash (`-`) is three times the duration of a dot (`.`).
- The gap between components of a letter has the same duration as a dot.
- The gap between digits has the same duration as a dash.
- The duration of the gap between repeating codes is seven times the duration of a dot.

The numbers of dots/dashes and the Morse code equivalent is shown in the table below.

Colour	Digits	Dots and dashes	Morse code	Meaning
Red	1-1-1	. - .	E T E	Battery voltage out of spec
Red	1-2-1	. - - .	E M E	Crypto SerDes core voltage out of spec
Red	1-2-2	. - - . .	E M I	Main processor SerDes core voltage out of spec
Red	1-2-3	. - - . . .	E M S	Main processor core voltage out of spec
Red	1-2-4	. - -	E M H	Main processor SerDes core IO voltage out of spec
Red	1-2-5	. - -	E M 5	Crypto SerDes IO voltage out of spec
Red	1-3-1	. - - - .	E O E	Main processor IFC IO voltage out of spec
Red	1-3-2	. - - - . .	E O I	DDR access voltage out of spec
Red	1-3-3	. - - - . . .	E O S	DDR IO voltage out of spec
Red	1-3-4	. - - -	E O H	V12 voltage out of spec
Red	1-3-5	. - - -	E O 5	Security processor voltage out of spec
Red	1-5-1	. - - - - - .	E 0 E	Security processor temperature out of spec
Red	1-5-2	. - - - - - . .	E 0 I	Main processor temperature out of spec
Red	1-5-3	. - - - - - . . .	E 0 S	Crypto temperature out of spec
Red	1-5-4	. - - - - -	E 0 H	Security processor app blank
Red	1-5-5	. - - - - -	E 0 5	Security processor app invalid
Red	2-1-1	. . - .	I T E	Security processor secure state corrupted
Red	2-1-2	. . - . .	I T I	No bootloader heartbeat
Red	2-1-3	. . - . . .	I T S	Board-ID PROM failed
Blue	2-1-5	. . -	I T 5	Firmware signature auth failure
Red	2-2-2	. . - - . .	I M I	Crypto known-answer tests failed
Red	2-2-3	. . - - . . .	I M S	RNG driver failed
Red	2-2-4	. . - -	I M H	FIPS DRBG failed
Red	2-2-5	. . - -	I M 5	OpenSSL failed
Red	2-3-1	. . - - - .	I O E	OpenSSH failed
Red	2-3-2	. . - - - . .	I O I	Library signature verification failed
Red	2-3-3	. . - - - . . .	I O S	FPGA initialisation failed
Red	2-3-4	. . - - -	I O H	Init script failed

10.3. Error codes accessed remotely

If an HSM enters an error state, you can retrieve error codes using the `enquiry` utility. These codes appear in the `hardware status field` of the `Module` and are included in the hardserver log.

There are three error categories:

- Runtime library errors.
- Hardware driver errors.
- Operational mode errors.

Error codes are also indicated by the LED on the back of the HSM, see LED error states.

10.3.1. Runtime library errors

The runtime library error codes described in the following table indicate one of the following:

- There is a bug in the firmware.
- There is a hardware fault.

If any of these errors occur, reset the HSM.

Code	Meaning
O L C	SIGABRT: assertion failure and/or `abort()` called.
O L D	Interrupt occurred when disabled. This is more likely to indicate a hardware problem than a firmware problem.
O L E	SIGSEGV: access violation. This is more likely to indicate a hardware problem than a firmware problem.
O L J	SIGFPE: unsupported arithmetic exception (such as division by 0).
O L K	SIGOSERROR: runtime library internal error.
O L L	SIGUNKNOWN: invalid signal raised.

10.3.2. Hardware driver errors

The hardware driver error codes described in the following table indicate one of the following:

- Some form of automatic hardware detection has failed.
- There is a bug in the firmware.
- The wrong firmware has been loaded.

If any of these errors is indicated, contact Entrust Support.

Code	Meaning
H L	M48T37 NVRAM (or battery) failed.
H C V	CPLD wrong version for PCI policing firmware.
H C X	No crypto offload hardware detected.
H P P	PCI Interface Policing failure.
H V	Environment sensors failed. For example, the temperature sensor.
H D	Failure reading unique serial number.
H R	Random number generator failed.
H R F O	FIPS continuous RNG failed.
H R A O	Periodic RNG test failed.
H R S	RNG startup failed.
H R T	RNG selftest failed.
H R T P	Periodic (scheduled daily) RNG selftest failed.
H R M	RNG data matched.
H R Z	Impossible RNG Failure (match after PRNG).
H S S	Security processor internal semaphore error.
H O	Token interface initialization failed.
H E	EEPROM failed on initialization.
H C	Processing thread initialization failed.
H C P	Card poll thread initialization failed.
H F	Starting up crypto offload.
H C V	CPLD version number incorrect.
H J V	IPC-watcher failed.
H J U	IPC-EPD failed.
H J R	Module reset notification failed.
K R	RSA selftest failed.

Code	Meaning
H H D	Unique serial number detection failed.
H H P	PCI bus hardware detection failed.
H H R	RTC hardware detection failed or random number generator detection failed.
H S C	Error writing correct SOS message.

10.3.3. Operational mode errors

The runtime library error codes described in the following table indicate one of the following:

- There is a bug in the firmware.
- There is a hardware fault.

Code	Meaning	Action
T	Temperature of the HSM has exceeded the maximum allowable.	Restart your host computer, and improve HSM cooling. For the cooling requirements for your HSM, see the *Installation Guide*.
D	Fail command received.	Reset HSM by turning it off and then on again.
G G G	Failure when performing `ClearUnit` or `Fail` command.	Contact Entrust Support.
I J A	Audit logging: failed to send audit log message. This can occur for any type of log message. That is, a log message, signature block or certifier block.	Contact Entrust Support.
I J B	Audit logging: no module memory (therefore failed to send audit log message).	Contact Entrust Support.
I J C	Audit logging: key problem or FIPS incompatibility (therefore failed to sign audit log message).	Contact Entrust Support.
I J D	Audit logging: NVRAM problem (therefore failed to configure or send audit log message).	Contact Entrust Support.

11. Uninstalling existing software

Entrust recommends that you uninstall any existing older versions of Security World Software before you install new software. In Windows environments, if the installer detects an existing Security World Software installation, it asks you if you want to install the new components. These components replace your existing installation.

The automated Security World software installers do not delete user created components, key data, or Security World data. However, on Linux, a manual installation using `.tar` files *does* overwrite existing data and directories.

Before you uninstall the Security World Software, Entrust strongly recommends that you make a secure backup of any existing Security World and nShield configuration files. See the *User Guide* for more information.

Entrust recommends that you take a backup of your `sshadmin` key using `hsmadmin keys backup` (for keys that will be used on the same machine) or `hsmadmin keys backup --passphrase` (for keys that may be transferred to another machine) before uninstalling or deleting any software or data. If you erase your SSH keys without a backup, you will need to use recovery mode to recover your module which will return the HSM to factory state.

When upgrading the Security World Software, you do NOT need to delete key data or any existing Security World. If you want to do so for other reasons, see the *User Guide* for your module and operating system for more information. If you do delete Security World data, it cannot be restored unless you have an up-to-date backup and a quorum of the Administrator Card Set (ACS) is available.

The file `nCipherKM.jar`, if present, is located in the `extensions` folder of your local Java Virtual Machine. The uninstall process may not delete this file. Before reinstalling over an old installation, remove the `nCipherKM.jar` file. See the *User Guide* for your module and operating system for more about locating the Java Virtual Machine `extensions` folder.

You can only have a single Security World Software installation on a computer at a time

If you are downgrading a software authenticated client to a Security

World Software earlier than version 12.60, the client will need to be re-enrolled as software-based authentication is not supported. See the *Configuring the nShield Connect to use the client* section in the *nShield Connect User Guide* for more information.

Entrust recommends that you do not uninstall the Security World Software unless you are either certain it is no longer required, or you intend to upgrade it.

11.1. Uninstalling the Security World Software on Windows

Before uninstalling the Security World software, you should back up your `%NFAST_HOME%` directory. Delete this backup after upgrading the Security World and confirming that the configuration files and any customizations are correct.

1. Open the **Control Panel** and select **Programs and Features**.
2. For the following programs, select **Uninstall** and follow the on-screen instructions:
   - **nShield Security World Software**
   - **CyberJack Base Components**

11.2. Uninstalling the Security World Software on Linux

Before uninstalling the Security World software, back up your `$NFAST_HOME` directory. This preserves your key management data, `hardserver.d`, and any data customizations.

When upgrading the Security World, restore the backup to preserve your PKCS #11 and Soft KNETI authentication settings and any customizations. If you delete the `/opt/nfast` directory without making a copy of it, you will lose these configuration settings.

When restoring a Security World from a backup, you need to maintain permissions.

If you are doing a clean reinstallation of the Security World software, ensure you backup the following files and folders before uninstalling:

- `/opt/nfast/kmdata`
- Your SSH keys in `/opt/nfast/services` (using `hsmadmin keys backup`).

Do not delete `/etc/nfast/config` nor the `nfast` and `ncsnmpd` users.

1. Assume the nFast Administrator privileges or root privileges by running the command:

```
$ su -
```

2. Type your password, then press **Enter**.
3. To remove drivers, install fragments, and scripts and to stop services, run the command:

```
/opt/nfast/sbin/install -u
```

4. Delete all the files (including those in subdirectories) in `/opt/nfast` and `/dev/nfast/` by running the following commands:

```
rm -rf /opt/nfast
rm -rf /dev/nfast
```

5. If you are not reinstalling the product, delete the configuration file `/etc/nfast.conf` if it exists.
6. Unless needed for a new installation, remove the user `nfast` and, if it exists, the user `ncsnmpd` using `sudo userdel` and `sudo groupdel`. For example:

```
sudo userdel ncsnmp
sudo userdel nfast
sudo groupdel ncsnmp
sudo groupdel nfast
```

If required, you can safely remove the module after shutting down all connected hardware.

12. Software packages on the Security World installation media

This appendix lists the contents of the component bundles and the additional software sup plied on your Security World Software installation media. For information on installing the supplied software, see Installing the software.

Entrust supply the hardserver and associated software as bundles of common components that provide much of the required software for your installation. In addition to the compo- nent bundles, provide individual components for use with specific applications and features supported by certain Entrust modules.

To list installed components, use the `ncversions` command-line utility.

12.1. Security World installation media

The following component bundles and additional components are supplied on the Security World installation media:

12.1.1. Component bundles

Linux Package	Windows Feature in the Installer	Content
`hwsp`	nShield Hardware Support	Hardware Support package, including the nShield Server and device driver.
`ctls`	nShield Core Tools	Management utilities, including generatekey, diagnos- tic and performance tools, Remote Administration Client cmd, and the PKCS#11 library.
`ctd`	nShield Cipher Tools	Developer package example programs, and developer libraries for the nCore API and generic stub.
`devref`	nShield Developer Reference	Reference Documentation for the nCore API.
N/A	nShield CSPs (CAPI, CNG)	CAPI and CNG providers and associated tools.
N/A	nShield Debug	PDB and .map files for nShield libraries and executa- bles.
N/A	nShield Device Drivers	Device drivers for PCI and USB attached nShield devices, included in `hwsp` for Linux.
`javasp`	nShield Java	nCipherKM JCA/JCE Provider, associated classes (including nFast Java generic stub classes) and the KeySafe application.

Linux Package	Windows Feature in the Installer	Content
`jd`	nShield Java Developer	Java developer libraries and documentation for the nCore API and generic stub.
`ncsnmp`	nShield SNMP	nShield SNMP service and tools.
N/A	nShield Remote Administration Client Tools	Remote Administration Client tools and shortcuts.
N/A	nShield Trusted Verification Device	Driver for the Trusted Verification Device (TVD), included in `ctls` for Linux.
`raserv`	nShield Remote Administration Server	nShield Remote Administration server for enabling communication between remote clients and their Type3 smartcards and this machine.
`redist`	N/A	Contains the redistributable GNU C and C++ shared libraries.

12.2. Components required for particular functionality

Some functionality requires particular component bundles or individual components to be installed.

Support for nShield Edge is shipped by default as part of the nShield Hardware Support component.

Ensure that you have installed the **Hardware Support (mandatory)** and **Core Tools (mandatory)** components.

In these part codes, *n* represents any integer.

If you are developing in Java, install the **Java Developer** and **Java Support (including KeySafe)** bundles; after installation, ensure that you have added the `.jar` files to your `CLASSPATH`.

You must install the `hwsp` component if you are using an nShield PCI card.

12.2.1. KeySafe

To use KeySafe, install the nShield **Core Tools** (`ctls` on Linux) and the nShield **Java** (`javasp` on Linux) components.

12.2.2. Microsoft CAPI CSP and Microsoft Cryptography API: Next Generation (CNG)

If you require the Microsoft CAPI CSP, you must install the nShield CSPs (CAPI, CNG) component.

If you want to use the module with PKCS #11 applications, including release 4.0 or later of Netscape Enterprise Server, Sun Java Enterprise System (JES), or Netscape Certificate Server 4, install the nShield PKCS11 library. For detailed PKCS #11 configuration options, see:

- The appropriate *User Guide* for your module and operating system
- The appropriate third-party integration guide for your application

Integration guides for third-party applications are available from https://nshieldsupport.entrust.com.

12.3. nCipherKM JCA/JCE cryptographic service provider

If you want to use the nCipherKM JCA/JCE cryptographic service provider, you must install:

- The nShield Java bundle

An additional JCE provider `nCipherRSAPrivateEncrypt` is supplied that is required for RSA encryption with a private key. To install and use this provider, ensure that the `nCipherKM.jar` is in your `CLASSPATH` or `MODULEPATH`. You will also need to add the following classname to the top of the list of providers in your `java.security` file `com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt`

See the *User Guide* for your module and operating system for more about configuring the nCipherKMJCA/JCE cryptographic service provider.

12.4. SNMP monitoring agent

If you want to use the **SNMP monitoring agent** to monitor your modules, install the nShield SNMP component (`ncsnmp` on Linux).

During the first installation process of the SNMP agent, the agent displays the following message:

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

See the *User Guide* for your module and operating system for more about how to activate the SNMP agent after installation.