nShield Security World

nToken v12.40 Installation Guide

04 March 2024

Contents

Chapter 1: Introduction

The nToken increases the security of the connection between the client computer and an HSM, by proving to the HSM that the client is in possession of a hardware token that cannot be cloned.

About this guide

This guide includes:

- Installing the nToken. See *Chapter 5: Installing the module* on page 16.
- Installing the Security World Software. See *Chapter 7: Installing the software* on page 20.
- A description of the module status indicators. See *Chapter 8: Status indicators* on page 26.
- Instructions about removing existing software. See *Appendix A: Uninstalling existing software* on page 30.

See the User Guide for more about, for example:

- Creating and managing a Security World
- Creating and using keys
- Card sets

For information on integrating nCipher products with third-party enterprise applications, see https://www.ncipher.com/resources.

Model Numbers

The table below shows the different versions of the module. The letter *x* represents any single-digit integer.

Model number	Used for
xC2021E-000 and xC2023E-000	nCipher nToken module with a PCI Express (PCIe) interface.

Note: nToken PCIe model number xC2021E-000 is not compatible with AIX and HP-US operating systems. For these operating systems nCipher recommend nToken PCIe model number xC2023E-000.

Additional documentation

You can find additional documentation in the **`document`** directory of the installation media for your product.

For information about using the software, see the *nShield Connect User Guide*.

See the User Guide for a glossary of terms.

nCipher strongly recommends that you read the release notes in the **`release`** directory of your installation disc before you use the module. These notes contain the latest information about your product.

Typographical conventions

Note: The word **Note** indicates important supplementary information.

Pay particular attention to any warnings and cautions accompanied by the following symbols:


Risk of electric shock to the user


Risk of damage to the module


Risk of static damage to the module


Risk of losing critical security parameters

Chapter 2: Hardware security modules

Power requirements

Module	Maximum power
PCIe	9.9W

Note: Ensure that the power supply in your computer is rated to supply the required electric power.

The PCIe card 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.

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 PCIe connector 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.

Environmental requirements

When you install the module, ensure that there is good air flow around it. To maximize air flow, use a PCIe slot with no neighboring modules if possible. If air flow is limited, consider fitting extra cooling fans to your computer case.

⚠ Failure to provide adequate cooling can result in damage to the module or the computer into which the module is fitted.

Always handle the module correctly. For more information, see *Handling modules* on page 8.

Module operational temperature and humidity specifications

The PCIe module operates within the following environmental conditions.

PCIe environmental conditions	Operating range		Comments
	Min.	Max.	
Ambient operating temperature	10°C	35°C	Subject to sufficient air flow
Storage temperature	-20°C	70°C	-
Operating humidity	10%	90%	Relative. Non-condensing at 35°C
Storage humidity	0	85%	Relative. Non-condensing at 35°C

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

Cooling requirements

Adequate cooling of the module is essential for trouble-free operation and a long operational life.

During operation you can use the supplied **stattree** utility to check the actual and maximum temperature of the module. 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. If the module exceeds the safe operating temperature, it stops operating and displays the **SOS-T** error message on the Status LED (see *Status indicators* on page 26).

Physical location considerations

nCipher nShield HSMs are certified to NIST FIPS 140-2 level 2 and 3. 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.

Chapter 3: Regulatory notices

FCC class A notice

This nShield Solo HSM complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This 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 user will be required to correct the interference at his own expense.

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

Recycling and disposal information

A Takeback and Recycle program is provided in compliance with the Waste Electrical and Electronic Equipment (WEEE) directive for the recycling of electronic equipment. The program enables you to return an obsolete or surplus nCipher Security product, which is then disposed of in an environmentally safe manner. For further information or to arrange the safe disposal of your product, e-mail recycling@ncipher.com.

Avis juridiques

Classe A de la FCC

Ce HSM Solo nShield répond aux exigences de la partie 15 du règlement de la FCC. Le fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne peut pas causer d'interférence nuisible, et
2. Cet appareil doit accepter toute interférence reçue, incluant les interférences qui peuvent causer un fonctionnement non désiré.

Cet équipement a été testé et respecte les limites pour les appareils numériques de classe A, selon la partie 15 du règlement de la FCC. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nuisibles lorsque l'équipement fonctionne dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie radio fréquence et, s'il n'est pas installé et utilisé conformément au manuel d'instruction, peut causer des interférences nuisibles à la radiocommunication. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de causer des interférences nuisibles auquel cas l'utilisateur devra corriger les interférences à ses propres frais.

Certification canadienne - CAN ICES-3 (A)/NMB- 3(A)

Information concernant le recyclage et le traitement

Un programme Take Back et Recycle (Rapportez et Recyclez) est fourni conformément à la directive Waste Electrical and Electronic Equipment (WEEE) pour le recyclage des équipements électroniques. Le programme vous permet de rapporter vos produits nCipher Security obsolètes ou en excédent, qui seront ensuite traités dans le respect de l'environnement. Pour plus d'informations ou pour organiser le traitement sûr de vos produits, envoyez un courriel à recycling@ncipher.com.

Rechtliche Informationen

Hinweis FCC-Klasse A

Das nShield Solo-HSM erfüllt die Anforderungen von Teil 15 der FCC-Bestimmungen. Der Betrieb des Geräts unterliegt den folgenden zwei Bedingungen:

1. Das Gerät darf keine störenden Interferenzen verursachen, und
2. Dieses Gerät muss störenden Interferenzen, die auf das Gerät auftreffen, widerstehen (einschließlich Interferenzen, die einen ungewollten Betrieb verursachen).

Dieses Gerät wurde gemäß Teil 15 der FCC-Bestimmungen getestet und erfüllt die Grenzwerte für Digitalgeräte der Klasse A. Diese Grenzwerte sollen einen geeigneten Schutz gegen störende Interferenzen bereitstellen, wenn das Gerät in einer industriellen Umgebung betrieben wird. Dieses Gerät erzeugt, nutzt und kann Hochfrequenzenergie ausstrahlen und kann, sofern es nicht gemäß den Anweisungen im Nutzerhandbuch installiert und verwendet wird, Funkverbindungen stören. Der Betrieb dieses Geräts in Wohngegenden kann möglicherweise störende Interferenzen verursachen. In einem solchen Fall muss der Nutzer die Interferenzen auf seine eigenen Kosten abstellen.

Kanadische Zertifizierung - CAN ICES-3 (A)/NMB- 3(A)

Informationen zu Recycling und Entsorgung

Gemäß der WEEE-Richtlinie (Waste Electrical and Electronic Equipment) wird zur Wiederverwertung von elektronischen Geräten ein Rücknahme- und Recyclingprogramm wird bereitgestellt. Im Rahmen dieses Programms können Sie veraltete oder nicht mehr genutzte nCipher Security Produkte zurückgeben, die dann umweltfreundlich entsorgt werden. Für weitere Informationen oder um die sichere Entsorgung Ihres Produkts zu veranlassen, senden Sie uns eine E-Mail an recycling@ncipher.com.

Notificaciones reglamentarias

Notificación clase A de la FCC

Este HSM nShield Solo cumple con la parte 1 5 de la reglamentación de la Comisión Federal de Comunicaciones (Federal Communications Commission, FCC) La operación está sujeta a las dos siguientes condiciones:

1. Este dispositivo no debe causar interferencia dañina, y
2. El dispositivo debe aceptar cualquier interferencia recibida, incluyendo aquella que pueda causar operaciones indeseadas.

Este equipo ha sido probado y se ha encontrado que cumple los límites para dispositivos digitales Clase A, según la parte 15 de la reglamentación de la FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias dañinas cuando el equipo opere en un ambiente comercial. Este equipo genera, utiliza y puede emitir energía de radiofrecuencia y, de no ser instalado y utilizado de acuerdo con el manual de instrucciones, puede causar interferencia dañina a las radiocomunicaciones. Es probable que la operación de este equipo en un área residencial cause interferencia dañina, y en este caso el usuario está obligado a remediar la interferencia por sus propios medios.

Certificación de Canadá - CAN ICES-3 (A)/NMB- 3(A)

Información de desecho y reciclaje

Se proporciona un programa de Devolución y Reciclaje que cumple con la directiva de Residuos de Aparatos Eléctricos y Electrónicos (Waste Electrical and Electronic Equipment directive, WEEE) para el reciclaje de equipo electrónico. El programa le permite devolver un producto de nCipher Security obsoleto o sobrante, que luego es desechado de forma segura para el medio ambiente. Por más información o para organizar el desecho seguro de su producto, envíe un correo electrónico a nCipher Support.

Chapter 4: Before installing the module

Module pre-installation steps

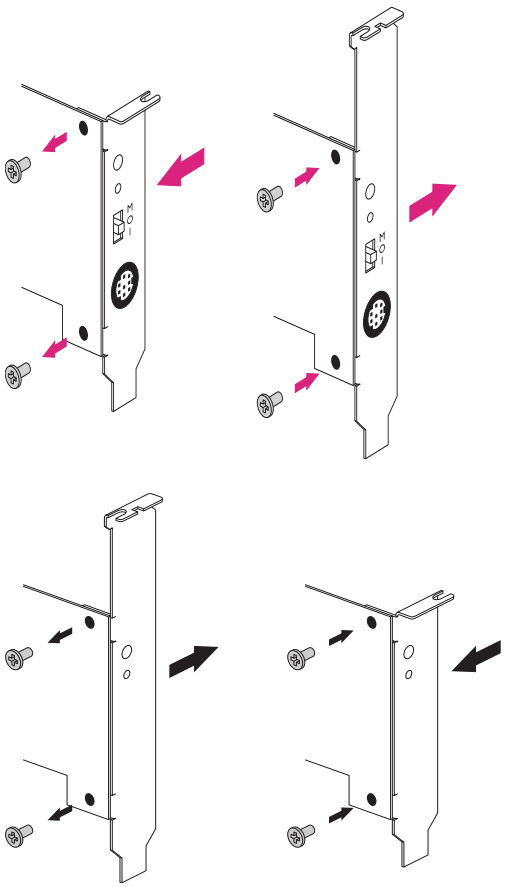
Check the module to ensure that there is no sign of damage or tampering:

- Check the epoxy resin security coating or metal lid of the module for obvious signs of damage.

Fitting a module bracket

Do not touch the nShield Solo connector pins, or the exposed area of the module without taking ESD precautions.

Figure 1. Removing the low profile bracket (left) and fitting the full height bracket (right)



To fit the full height bracket to the module:

Chapter 5: Installing the module

To install the module:

1. Power off the system and while taking ESD precautions, remove the PCIe card.
2. Open the computer case and locate an empty PCIe slot. If necessary, follow the instructions that your computer manufacturer supplied.

Do not install a PCIe module into a PCI slot. See the instructions that your computer manufacturer supplied to correctly identify the slots on your computer.

Note: 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.

5. 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
6. Use the bracket screw or fixing clip to secure the module to the computer chassis.
7. Replace the computer case.

After installing the module

Note: After you install the module, check regularly to ensure that it has not been tampered with during operation.

After you install the module, you must install the Security World 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.

Chapter 6: Before you install the software

- Uninstall any older versions of Security World Software. See *Appendix A: Uninstalling existing software* on page 30.

Preparatory tasks before installing software

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

Windows environments

Power saving options

Adjust your computers power saving setting to prevent sleep mode.

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/.

Unix Environments

Install operating environment patches

Make sure that you have installed the latest recommended patches. See the documentation supplied with your operating environment for information.

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.

All environments

Install Java with any necessary patches

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

- Java5 (or Java 1.5x)
- Java6 (or Java 1.6x)
- Java7 (or Java 1.7x)
- Java8 (or Java 1.8x).

We recommed 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 nCipher 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 nCipher software, please contact nCipher support.

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 are:

Operating System	Download site
AIX	http://www.ibm.com/developerworks/systems/library/es-JavaOnAix_install.html
HPUX	https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJAVAHOME
various	http://www.oracle.com/technetwork/java/index.html
various	http://www.oracle.com/technetwork/java/all-142825.html

Note: You must have Java installed to use KeySafe.

Identify software components to be installed

nCipher 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.

Note: In Windows environments, you *must* install the **Hardware Support bundle**. If the **Hardware Support bundle** is not installed, your module cannot function.

Note: In Windows environments, the **Windows device drivers** component is installed as part of the **Hardware Support bundle**. In Unix environments, the **Kernel device drivers** component is installed.

Note: In Unix environements, you *must* install the `nfdrv` component.

nCipher recommends that you always install the **Core Tools bundle**. This bundle contains all the Security World Software command-line utilities, including:

- `generatekey`
- Low level utilities
- Test programs

Note: 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.

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	Use
Hardserver	9000	Internal non-privileged connections from Java applications including KeySafe
Hardserver	9001	Internal privileged connections from Java applications including KeySafe
Hardserver in nShield Connect	9004	Incoming impath connections from client machines

Chapter 7: Installing the software

This chapter describes how to install the Security World Software on the computer , client, or RFS associated with your nShield HSM.

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 more about creating a Security World and the appropriate card sets, and further configuration or setup tasks.

Installing the Security World Software

Installing Security World Software in a Windows environment

Do the following:

1. Log in as Administrator or as a user with local administrator rights.
2. Place the Security World Software installation media in the optical disc drive. Launch `setup.exe` manually if the installer does not run automatically.
3. Follow the onscreen instructions. Accept the license terms.
4. Select all the components required for installation, and then click **Next**. See *Appendix B: Components on Security World Software installation media (Windows and Unix)* on page 35 for more about the component bundles and the additional software supplied on your installation media.
   The selected components are installed in the default directory. The installer creates links to the following nShield Cryptographic Service Provider (CSP) setup wizards under **Start** > **All Programs** > **nCipher**:
   - **nCipher CSP install wizard**, which sets up CSPs for 32-bit applications
   - **nCipher 64bit CSP install wizard**, which sets up CSPs for 64-bit applications
6. The installer advises you that the SNMP agent does not run by default. Click **Next** to continue.
7. The installer advises you if you have an existing PKCS #11 installation. Click **Next** to continue.
8. The Security Assurance Mechanism (SAM) for the PKCS #11 library is selected by default. Select **No** if you want to disable the SAM. Click **Next** to continue. See the User Guide for more about the SAM and the available configuration options.
9. Click **Finish** to complete the installation.
10. Update your system environment `PATH` by inserting the sub-path `%NFAST_HOME%\bin`.

Installing Security World Software in a Unix Linux environment

Installing on Solaris

To install the Security World Software for Solaris:

1. Log in as a user with root privileges.
2. Place the installation media in the optical disc drive, and mount the drive.

3. To install the Security World Software server, run the command:

```
/usr/sbin/pkgadd -d /cdrom/disc-name/solaris/ver/type/nfast/nfast.pkg
```

   In this example, `disc-name` is the mount point of the installation media, `ver` is the version of Solaris (for example, use **11** for Solaris version 11) and `type` is **amd64** for Solaris x86 and **sparc** for Solaris Sparc.

4. From the list of packages available for installation, select all required packages, press `Enter` and follow the on-screen instructions.
5. Run the install script by using the following command:

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

   After the software is installed, you are returned to the shell prompt.

6. 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
```

Installing on AIX

To install the Security World Software for AIX:

1. Log in as a user with root privileges.
2. Place the installation media in the optical disc drive, and mount the drive.
3. Start the software management tool by running the command:

```
smit install_latest
```

4. Select **List** to display the input device or directory for the software, and select the location that contains the installation image.
5. For **SOFTWARE to install**, select **List**, and then select all required file sets See *Appendix B: Components on Security World Software installation media (Windows and Unix)* on page 35 for more about the component bundles and the additional software supplied on your installation media.

6. Press `Enter` to confirm the file set selection.

   When additional installation options are displayed, leave the default settings enabled. Press `Enter` to confirm these settings, and then press `Enter` again to begin the installation.

7. After software installation is complete, run the install script with the following command:

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

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
     ```

Installing on HP-UX

To install the Security World Software for HP-UX:

1. Log in as a user with root privileges.
2. Place the installation media in the optical disc drive, and mount the drive, using the **`-o cdcase`** option.
3. Open a terminal window, and start the software management tool by running a command of the form:

   ```
   swinstall -s disc-name/hpux/ver/nfast/nfast.dep
   ```

   In this example, `disc-name` is the mount point of the installation media and `ver` is the version of HP-UX (for example, use **11_31** for HP-UX version 11.31).

4. Select all the required software bundles and components for installation.
5. Select **Install** from the **Actions** menu.
6. When the installation analysis is complete, click **OK**. If the installer reports any errors, click **Logfile** to display them.
7. Click **Yes** to confirm you want to install.
8. The installer now installs the selected products. When it is complete, click the **Done** button.
9. Log in as **`root`**.

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

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

11. 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
```

Installing on Linux

To install the Security World Software for Linux:

1. Log in as a user with root privileges.
2. Place the installation media in the optical disc drive, and mount the drive.
3. Open a terminal window, and change to the root directory.
4. Extract the required **`.tar`** files to install all the software bundles by running commands of the form:

```
tar xf disc-name/linux/ver/nfast/bundle/file.tar
```

In this command, *ver* is the version of the operating system (for example, **`libc6_11`**), *bundle* is the directory name of a given bundle (for example, **`hwsp`** or **`ctls`**), and *file*`.tar` is the name of a **`.tar`** file within a bundle directory.

Note: Some directories contain more than one **`.tar`** file.

5. To use an nShield module with your Linux system, you must build a kernel driver. nCipher supplies the source to the nCipher PCI kernel driver (**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:

   1. Change directory to the nCipher PCI driver directory by running the command:

      ```
      # cd /opt/nfast/driver/
      ```

   2. Configure the source by running the command:

      ```
      # ./configure
      ```

   3. 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. Log 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:

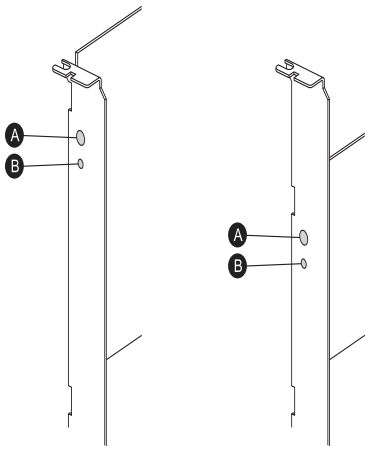
```
PATH=/opt/nfast/bin:$PATH
export PATH
```

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

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

Chapter 8: Status indicators

Figure 2. Back panel: PCIe module



Label	Description
A	Status LED
B	Recessed reset button

Status LED

The blue Status LED indicates the operational status of the module.

Status LED	Description
Off.	**`Status: Power off`** There is no power supply to the module. Check that the module is correctly inserted in its PCIe slot, then restart the computer.
On, occasionally blinks off.	**`Status: Operational mode`** The nSheild Solo module is accepting commands. The more frequently the Status LED blinks off, the greater the load on the module. .
Flashes SOS, the Morse code distress code (three short pulses, three long pulses, three short pulses). After flashing SOS, the Status LED flashes an error code in Morse code.	**`Status: Error mode`** If the module encounters an unrecoverable error, it enters Error mode. In Error mode, the module does not respond to commands and does not write data to the bus. If a command does not complete successfully, the module normally writes an error message to the log file and continues to accept further commands. It does not enter Error mode. For information about error codes, see the User Guide.

Chapter 9: Configuring and checking the installation

This section describes how to:

- Configure the nShield Connect so that it can recognize the nToken installed on the client computer.
- Check that the nToken is installed and configured correctly on the client.

Note: For more information about configuring an nShield Connect to use clients, see the *nShield Connect User Guide*.

Adding the client to the nShield Connect

When the client is added to the nShield Connect, the client must use the nToken to communicate with the nShield Connect. If the client attempts to connect to the nShield Connect when a module is in use, the nShield Connect examines the IP address of the client and requires the client to identify itself using the authentication key of the module.

To add the client to the nShield Connect:

1. Use the right-hand navigation button on the nShield Connect front panel to select **System > System configuration > Client configuration > New client**.
2. Enter the IP address and netmask of the first client, and press the right-hand navigation button.
3. To choose the permissions for the client, use the touch wheel to display the type of connection between the nShield Connect and the client. The table below lists the available options.

Option	Description
Unprivileged	Privileged connections are never allowed.
Priv. on low ports	Privileged connections are allowed only from ports numbered less than 1024. These ports are reserved for use by root on Unix-based systems.
Priv. on any ports	Privileged connections are allowed on all ports.

   Note: You need a privileged connection to perform module administration tasks (for example, to create a Security World). If you are not going to perform module administration tasks, we recommend that you allow only unprivileged connections. For more information, see the *nShield Connect User Guide*.

   When you have selected the type of connection, press the right-hand navigation button.
7. To enroll the client with an nToken, enter the number of the port on which the client is listening (the default is 9004) and press the right-hand navigation button.

8. Retrieve the ESN and authentication key hash of the nToken:
   a. Open a command window on the client. Navigate to the directory where the Security World Software has been installed, and enter the following command:

```
ntokenenroll -H
```

   c. The ESN of the nToken and the hash of the nToken authentication key are displayed. Write down the ESN and the hash, or ensure that you can see the module as you work on the client.
9. On the module, compare the ESN of the nToken and the hash of the nToken authentication key with the ESN and hash displayed on the following screen:

```
Client nnnnnnnnnn reported the key hash:
xxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxx
Is this EXACTLY right?
```

   If there is an exact match, select Yes, and press the right-hand navigation button to configure the client.
12. When you see the confirmation message, press the right-hand navigation button again.
13. To enroll the client with the nToken, run the following command:

```
nethsmenroll [--ntoken-esn esn-of-ntoken] [Options]
nethsm-IP [nethsm_ESN netHSM_HKNETI]
```

Checking the installation

To check that the module is installed and configured correctly on the client:

1. Log in as a user and open a command window.
2. Run the command:

```
enquiry
```

3. The following is an example of the output following a successful **enquiry** command:

```
Module ##:
enquiry reply flags  none
enquiry reply level  Six
serial number        ####-####-####-####
mode                 operational
version              #.#.#
speed index          ###
rec. queue           ##..##
...
rec. LongJobs queue  ##
SEE machine type     ARMtype2
supported KML types  DSAp1024s160 DSAp3072s256
```

If the **mode** is **operational** the module has been installed correctly.
If the output from the **enquiry** command says that the module is not found, first restart your computer, then re-run the **enquiry** command.

> **Note:** Under Windows 7 and Windows 2008 R2, ensure that the power saving features are disabled. See *Installing the module* on page 16 for more information. Otherwise, if your system enters Sleep mode, the nToken may not be found when running **enquiry**. If this happens, you need to reboot your system.

Appendix A: Uninstalling existing software

nCipher recommends that you uninstall any existing older versions of Security World Software before you install new software.

The automated Security World Software installers *do not* delete other components or any key data and Security World data that you have created.

The uninstaller removes only those files that were created during the installation.

Note: Before you uninstall the Security World Software, nCipher strongly recommends that you make a secure backup of any key data and any existing Security World. See the User Guide for more information.

Note: 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 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.

Note: 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.

Note: In Windows environments, because the hardserver is installed as a named service (known as the nFast server), it is only possible to have one Security World Software installation on any given computer.
It is also not possible to have more than one Security World Software installation on the same computer in Unix environments.

nCipher 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.

Uninstalling Windows software

To uninstall Security World Software in a Windows environment:

1. Open the **Control Panel** and click **Programs and Features**.
2. Select the Security World Software, click **Uninstall**, and follow the on-screen instructions.

Uninstalling Unix software

Uninstalling on Solaris

To uninstall the Security World Software from Solaris:

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. Remove the software package by running the command:

   ```
   /usr/sbin/pkgrm
   ```

   The command displays the list of components that were installed.

5. Select all the nShield packages (prefixed with the letters **NC**), then press `Enter`.
6. Follow the onscreen instructions, confirming the uninstallation of packages as prompted.
7. If you are not planning to re-install the product, delete the configuration file **`/etc/nfast.conf`** if it exists.

Note: Do not delete the configuration file if you are planning to re-install the product.

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

Uninstalling on AIX

To uninstall the Security World Software from AIX:

1. Log in as a user with root privileges.
2. To remove drivers, install fragments, and scripts and to stop services, run the command:

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

3. Start the software management tool by running the command:

```
smit install_remove
```

4. For **SOFTWARE name**, select **List** to list all available file sets, and then select all those prefixed with **ncipher**.
5. Press `Enter` to confirm the selected file sets for uninstallation.
   The **Remove Installed Software** panel is displayed.
7. Ensure that the **PREVIEW Only** option is set to **No** (or the removal operation does not occur), and press `Enter`.
8. When prompted to confirm that you are sure about the removal, press `Enter` again to start the uninstall process.
9. If you are not planning to re-install the product, delete the configuration file **`/etc/nfast.conf`** if it exists.

Note: Do not delete the configuration file if you are planning to re-install the product.

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

Uninstalling on HP-UX

To uninstall the Security World Software from HP-UX:

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. Remove the software packages by running the command:

```
/usr/sbin/swremove
```

   The command displays the list of components that were installed.

5. Select all the packages.
6. Select **Remove** from the **Actions** menu.
7. When the analysis is complete, if there are no errors, click **OK**. If the installer reports any errors, click **Logfile** to display them.
8. When the uninstaller asks you to confirm that you want to remove this product, click **Yes**.
9. When the uninstallation is complete, click **Done**.
10. If you are not planning to re-install the product, delete the configuration file **`/etc/nfast.conf`** if it exists.

Note: Do not delete the configuration file if you are planning to re-install the product.

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

Uninstalling on Linux

To uninstall the Security World Software from Linux:

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
```

   Note: Deleting all the files and subdirectories in **/opt/nfast** also deletes the **/opt/nfast/kmdata** directory. To be able to restore an existingSecurity World after deleting all the files in **/opt/nfast**, ensure you have made a backup of the **/opt/nfast/kmdata** directory in a safe location before deleting the original.

5. If you are not planning to re-install the product, delete the configuration file **/etc/nfast.conf** if it exists.

   Note: Do not delete the configuration file if you are planning to re-install the product.

6. Unless needed for a subsequent installation, remove the user **nfast** and, if it exists, the user **ncsnmpd**:
   a. Open the file **/etc/group** with a text editor.
   b. Remove the line that begins with the form:

```
nfast:x:n
```

      In this line, *n* is an integer.

   c. Open the file **/etc/passwd** with a text editor.
   d. Remove the line that begins with the form:

```
nfast:x:...
```

   e. If it exists, remove the line that begins with the form:

```
ncsnmpd:x:...
```

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

Appendix B: Components on Security World Software installation media (Windows and Unix)

This appendix lists the contents of the component bundles and the additional software supplied on your Security World Software installation media. For information on installing the supplied software, see *Installing the software* on page 20.

nCipher 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 component bundles, nCipher provide individual components for use with specific applications and features supported by certain nCipher modules.

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

Security World for nShield User installation media

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

Component bundles

Unix Package	Description (Windows and Unix)	Contents of bundle
hwsp	**Hardware Support** (mandatory)	See *Hardware support*
ctls	**Core Tools** (recommended)	See *Core tools*
javasp	**Java Support** (including KeySafe)	See *Java Support (including KeySafe)*
nhfw	**nShield Connect firmware files**	See *nShield Connect firmware files*
dsserv	**Remote Administration Service** (optional)	See *Remote Administration Service*
ratls	**Remote Administration Client** (optional) - Windows and Linux only	See *Remote Administration Client*

Individual components

Unix Package	Description (Windows and Unix)
	nCipher CAPI-NG providers and tools - Windows only
hwcrhk	**Crypto Hardware Interface (CHIL) plugin**
jcecsp	**nCipherKM JCA/JCE provider classes**
	CSP Console utilities - Windows only
	CryptoAPI CSP GUI and console installers - Windows only
ncsnmp	**Net-SNMP monitoring agent, utilities with nCipher MIB functionality**
pkcs11	**nCipher pkcs11 library**

CipherTools installation media

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

Component bundles

Unix Package	Description (Windows and Unix)	Contents of bundle
hwsp	**Hardware Support** (mandatory)	See *Hardware support*
ctls	**Core Tools** (recommended)	See *Core tools*
javasp	**Java Support** (including KeySafe)	See *Java Support (including KeySafe)*
ctd	**CipherTools Developer**	See *CipherTools Developer*
jd	**Java Developer**	See *Java Developer*
nhfw	**nShield Connect firmware files**	See *nShield Connect firmware files*
dsserv	**Remote Administration Service** (optional)	See *Remote Administration Service*
ratls	**Remote Administration Client** (optional) - Windows and Linux only	See *Remote Administration Client*

Individual components

Unix Package	Description (Windows and Unix)
	nCipher CAPI-NG providers and tools - Windows only
devref	**nCore API Documentation**
hwcrhk	**Crypto Hardware Interface (CHIL) plugin**
jcecsp	**nCipherKM JCA/JCE provider classes**
	CSP Console utilities - Windows only
	CryptoAPI CSP GUI and console installers - Windows only
ncsnmp	**Net-SNMP monitoring agent, utilities with nCipher MIB functionality**
pkcs11	**nCipher pkcs11 library**
sslyp	**Open SSL source code patch file**

CodeSafe installation media

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

Component bundles

Unix Package	Description (Windows and Unix)	Contents of bundle
hwsp	**Hardware Support** (mandatory)	See *Hardware support*
ctls	**Core Tools** (recommended)	See *Core tools*
javasp	**Java Support** (including KeySafe)	See *Java Support (including KeySafe)*
csd	**CodeSafe Developer**	See *CipherTools Developer*
jd	**Java Developer**	See *Java Developer*
nhfw	**nShield Connect firmware files**	See *nShield Connect firmware files*
dsserv	**Remote Administration Service** (optional)	See *Remote Administration Service*
ratls	**Remote Administration Client** (optional) - Windows and Linux only	See *Remote Administration Client*

Individual components

Unix Package	Description (Windows and Unix)
	nCipher CAPI-NG providers and tools - Windows only
csdref	**nCore CodeSafe API Documentation**
devref	**nCore API Documentation**
gccsrc	**Prebuilt arm-gcc for Codesafe/C**
gccsrc	**Prebuilt powerpcm-gcc for Codesafe/C**
hwcrhk	**Crypto Hardware Interface (CHIL) plugin**
jcecsp	**nCipherKM JCA/JCE provider classes**
	CSP Console utilities - Windows only
	CryptoAPI CSP GUI and console installers - Windows only
ncsnmp	**Net-SNMP monitoring agent, utilities with nCipher MIB functionality**
pkcs11	**nCipher pkcs11 library**

Common component bundles

nCipher supply component bundles containing many of the necessary components for your installation. Certain standard component bundles are offered for installation on all standard Security World Software installation media, while additional component bundles are found on CipherTools and CodeSafe installation media.

Common component bundles

You are always offered the following standard component bundles on all standard Security World Software installation media:

- Hardware Support
- Core Tools
- Java Support
- nShield Connect firmware files
- Remote Administration Service
- Remote Administration Client.

Hardware support

The **Hardware Support** (mandatory) bundle contains the hardserver and kernel device drivers:

Unix Package	Description (Windows and Unix)
	Windows device drivers - Windows only
nfserv	**Hardserver process executables and scripts**
sdrv	**nFast driver signatures**
cfgall	**Hardserver config file support**
nflog	**Logging library support**

Core tools

The **Core Tools** (recommended) bundle contains all the Security World Software command-line utilities, including `generatekey`, low level utilities, and test programs:

Unix Package	Description (WIndows and Unix)
`convrt`	`Command line key conversions`
`nftcl`	`Command line key management (Tcl)`
`nftcl`	`Command line key generation and import`
`nfuser`	`Low level utilities and test programs`
`nfuser`	`Command line remote server management`
`opensl`	`nftcl certificate generation utility`
`sworld`	`Command line key management (C)`
`tclsrc`	`Tcl run time`
`tclstf`	`Small Tcl utilities`
`nftcl`	`Command line key generation and import`
`tct2`	`Trusted Code Tool 2 command-line utility`
`pysrc`	`Python source for developers`
`nfpy`	

nCipher recommend that you always install the **Core Tools bundle**.

Note: The Core Tools bundle includes the `Tcl run time`'s tools for creating the Security World, `KeySafe`, and `new-world`. This does not affect any other installation of Tcl on your computer.

Java Support (including KeySafe)

The **Java Support (including KeySafe)** bundle contains Java applications:

Unix Package	Description (Windows and Unix)
`jutils`	`Java utilities`
`jutils`	`JNI shared library for jutils.jar`
`kmjava`	`Java Key Management classes`
`ksafe`	`KeySafe 2`
`nfjava`	`nFast Java generic stub classes`
`nftcl`	`Java Key Management Support`

Remote Administration Service

The Remote Administration Service bundle contains the Remote Administration Service installation and configuration. When installed, the Remote Administration Service starts automatically.

Remote Administration Client

Graphical User Interface and command line versions of the Remote Administration Client.

nShield Connect firmware files

Firmware image files for the nShield Connect. Typically a firmware image file is included that contains the latest FIPS Approved module firmware, as well as the firmware image file for the particular nShield release. In some cases these may be one and the same thing.

Additional component bundles

nCipher supply the following additional component bundles on CipherTools installation media:

- CipherTools Developer
- Java Developer.

nCipher supply the following additional component bundles on CodeSafe installation media:

- Code safe
- Java developer.

CipherTools Developer

The **CipherTools Developer** bundle contains components supplied with the CipherTools Developer Kit:

Unix Package	Description (Windows and Unix)
emvspj	JNI library for payShield Java
emvspp	payShield developer library
hwcrhk	Crypto Hardware Interface (CHIL) dev kit
nflibs	nCipher libraries and headers, and example C source for utility functions
nfuser	nCore & KM tools and example source
pkcs11	nFast PKCS#11 developer's library
sworld	Key Management C library developers kit
tclsrc	Tcl run time - Headers and Libraries
cutils	C utilities library
nflog	Logging library
hilibs	GS libs & headers
pysrc	Python source for developers
nfpy	nFPython header files

CodeSafe Developer

The **CodeSafe Developer** bundle contains components supplied with the CodeSafe Developer Kit:

Unix Package	Description (Windows and Unix)
csee	Codesafe-C moduleside example code
csee	Codesafe-C hostside example code
module	Firmware test scripts
nflibs	Generic stub libraries and headers, and example C source for utility functions
nfuser	nCore & KM tools and example source
sworld	Key Management C library developers kit
tclsrc	Tcl run time - Headers and Libraries
cutils	C utilities library
nflog	Logging library
hilibs	GS libs & headers
jhsee	Java hostside developer's kit
jhsee	Java hostside SEE examples
ssllib	Codesafe-SSL hostside code
ssllib	Codesafe-SSL moduleside code
pysrc	Python source for developers
nfpy	nFPython header files
nfpy	Libs and headers for codesafe/python

Java Developer

The **Java Developer** bundle contains components to support development of Java applications:

Unix Package	Description (Windows and Unix)
`jcecsp`	`Java Key Management developer`
`jutils`	`Java utilities source and javadocs`
`kmjava`	`Java Key Management developer`
`nfjava`	`Java Generic Stub examples & javadoc`

Components required for particular functionality

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

If you are planning to use Security World Software with an nShield Edge, ensure that the optional **Edge Monitor Controller** feature is selected during installation.

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

If you have CipherTools installation media, nCipher recommend that you install the **CipherTools Developer** bundle.

If you have CodeSafe installation media, nCipher recommend that you install the **CodeSafe Developer** bundle.

If you have CodeSafe installation media and you are developing in C:

- If your module has a part code of the form nC4*nn*2 or Bn1*nnn*, install the **Prebuilt arm-gcc for Codesafe/C** component.
- If your module has a part code of the form nC4*nn*3, Bn2*nnn*, BN2*nnn(-E)*, or NH2*nnn*, install the **Prebuilt powerpc-gcc for Codesafe/C** component.

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

If you have CipherTools installation media or CodeSafe installation media and 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 `nfdrvk` component if you are using a nCipher PCI card.

KeySafe

To use KeySafe, install the **Core Tools** and the **Java Support (including KeySafe)** bundles.

Microsoft CAPI CSP

If you require the Microsoft CAPI CSP, you must install the CSP components:

- **CSP console utilities**
- **CryptoAPI CSP GUI and console installers**

Microsoft Cryptography API: Next Generation (CNG)

If you require the Microsoft CNG, you must install the CNG component:

nCipher CAPI-NG providers and tools

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 **`nCipher 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 the nCipher web site: https://www.ncipher.com/resources/integration-guides.

Cryptographic Hardware Interface Library applications

If you want to use the module with the Cryptographic Hardware Interface Library (CHIL) applications, install the **Crypto Hardware Interface (CHIL) plugin** component and, if required, the **OpenSSL source code patch file** component.

Note: Security World Software supports OpenSSL 1.0.1g and later.

nCipherKM JCA/JCE cryptographic service provider

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

- The **Java Support (including KeySafe)** bundle
- The **nCipherKM JCA/JCE provider classes** component

An additional JCE provider **`nCipherRSAPrivateEncrypt`** is supplied that is required for RSA encryption with a private key. Install this provider and ensure that the file **`rsaprivenc.jar`** is in your **`CLASSPATH`**.

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

SNMP monitoring agent

If you want to use the SNMP monitoring agent to monitor your modules, install the **SNMP monitoring agent** component. During the first installation process of the SNMP agent, the agent displays the following message:

```
If this is a first time install, the nCipher 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.