



ENTRUST

nShield Security World

nShield Edge v12.50.4 Installation Guide

4 March 2024

Contents

| | |
|--|-----------|
| 1 Introduction | 7 |
| 1.1 About this guide | 7 |
| 1.2 Additional documentation | 8 |
| 1.2.1 Terminology | 8 |
| 1.3 Typographical conventions | 8 |
| 2 Safety and security | 9 |
| 2.1 FIPS | 10 |
| 3 Regulatory notices | 11 |
| 3.1 FCC class A notice | 11 |
| 3.2 Canadian certification - CAN ICES-3 (A)/NMB- 3(A) | 11 |
| 3.3 Recycling and disposal information | 11 |
| Avis juridiques | 12 |
| 3.4 Classe A de la FCC | 12 |
| 3.5 Certification canadienne - CAN ICES-3 (A)/NMB- 3(A) | 12 |
| 3.6 Information concernant le recyclage et le traitement | 12 |
| Rechtliche Informationen | 13 |
| 3.7 Hinweis FCC-Klasse A | 13 |
| 3.8 Kanadische Zertifizierung - CAN ICES-3 (A)/NMB- 3(A) | 13 |
| 3.9 Informationen zu Recycling und Entsorgung | 13 |
| Notificaciones reglamentarias | 14 |
| 3.10 Notificación clase A de la FCC | 14 |
| 3.11 Certificación de Canadá - CAN ICES-3 (A)/NMB- 3(A) | 14 |
| 3.12 Información de desecho y reciclaje | 14 |
| 4 Before you install the software | 15 |
| 4.1 Preparatory tasks before installing software | 15 |
| 4.1.1 Windows environments | 15 |
| 4.1.1.1 Install Microsoft security updates | 15 |

| | |
|---|-----------|
| 4.1.2 Unix Environments | 15 |
| 4.1.2.1 Install operating environment patches | 15 |
| 4.1.2.2 Users and Groups | 15 |
| 4.1.3 All environments | 16 |
| 4.1.3.1 Install Java with any necessary patches | 16 |
| 4.1.3.2 Identify software components to be installed | 16 |
| 4.2 Firewall settings | 17 |
| 5 Installing the software | 18 |
| 5.1 Installing the Security World Software | 18 |
| 5.2 Installing Security World Software in a Windows environment | 18 |
| 5.3 Installing Security World Software in a Linux environment | 19 |
| 5.3.1 Installing on Linux | 19 |
| 6 Setting up the nShield Edge | 20 |
| 6.1 Power saving options | 20 |
| 6.2 Connecting an nShield Edge | 20 |
| 6.2.1 Windows | 20 |
| 6.2.2 Linux | 20 |
| 6.3 Enabling optional features | 21 |
| 6.4 Disconnecting and reconnecting the nShield Edge | 21 |
| 6.5 Checking the installation | 22 |
| 6.6 Using a Security World | 22 |
| 7 Using the nShield Edge | 23 |
| 7.1 Mode LEDs | 24 |
| 7.2 Changing the mode | 24 |
| 7.3 Status LED | 24 |
| 8 Troubleshooting | 25 |
| 8.1 None of the LEDs are lit | 25 |
| 8.2 The Mode LED is amber or red | 25 |
| 8.3 The Status LED is flashing irregularly and the nShield Edge is unresponsive for more than a few minutes | 25 |
| 8.4 The Security World Software does not detect the connected nShield Edge | 25 |

| | |
|---|-----------|
| 8.5 Upgrading the firmware | 25 |
| 8.5.1 Contacting nCipher Support | 25 |
| 9 nShield Edge Windows compatibility issues and considerations | 26 |
| 9.1 nShield Edge very slow in VMware virtual machine | 26 |
| 10 Dimensions and operating conditions | 27 |
| 10.1 Physical location considerations | 27 |
| Appendix A Uninstalling existing software | 28 |
| A.1 Uninstalling Windows software | 28 |
| A.2 Uninstalling Unix software | 29 |
| A.2.1 Uninstalling on Linux | 29 |
| Appendix B Components on Security World Software installation media (Windows and Unix) | 31 |
| B.1 Security World for nShield User installation media | 31 |
| B.1.1 Component bundles | 31 |
| B.1.2 Individual components | 32 |
| B.2 CipherTools installation media | 32 |
| B.2.1 Component bundles | 32 |
| B.2.2 Individual components | 33 |
| B.3 CodeSafe installation media | 33 |
| B.3.1 Component bundles | 33 |
| B.3.2 Individual components | 34 |
| B.4 Common component bundles | 35 |
| B.4.1 Common component bundles | 35 |
| B.4.1.1 Hardware support | 35 |
| B.4.1.2 Core tools | 36 |
| B.4.1.3 Java Support (including KeySafe) | 36 |
| B.4.1.4 Remote Administration Service | 37 |
| B.4.1.5 Remote Administration Client | 37 |
| B.4.1.6 nShield Connect firmware files | 37 |
| B.4.2 Additional component bundles | 37 |
| B.4.2.1 CipherTools Developer | 38 |

| | |
|---|----|
| B.4.2.2 CodeSafe Developer | 39 |
| B.4.2.3 Java Developer | 40 |
| B.5 Components required for particular functionality | 40 |
| B.5.1 KeySafe | 41 |
| B.5.2 Microsoft CAPI CSP | 41 |
| B.5.3 Microsoft Cryptography API: Next Generation (CNG) | 41 |
| B.6 Cryptographic Hardware Interface Library applications | 41 |
| B.7 nCipherKM/JCA/JCE cryptographic service provider | 42 |
| B.8 SNMP monitoring agent | 42 |

1 Introduction

The nShield® Edge is a portable Hardware Security Module (HSM) for use in root Certification Authorities (CAs) and Registration Authorities (RAs), code signing, and remote HSM operations. The nShield Edge combines a full-featured HSM with a smart card reader, which you can use to securely store and access your organization's high-value occasional-use keys, such as certificate signing keys.

The nShield Edge has been designed and tested for deployments where one HSM is used with one computer or Windows Virtual Machine (VM). Multiple-unit deployments, where multiple nShield Edge HSMs are connected to the same computer or VM, are not supported.

We do not recommend using the nShield Edge alongside other nCipher HSMs on the same computer or VM.

1.1 About this guide

This guide includes:

- Installing the Security World Software. See *Installing the software* on page 18.
- Steps to set up an nShield Edge. See *Setting up the nShield Edge* on page 20.
- How to use an nShield Edge. See *Using the nShield Edge* on page 23.
- Troubleshooting information. See *Troubleshooting* on page 25.
- nShield Edge compatibility considerations. See *nShield Edge Windows compatibility issues and considerations* on page 26.
- Instructions to uninstall existing software. See *Uninstalling existing software* on page 28.
- Software components and bundles. See *Components on Security World Software installation media (Windows and Unix)* on page 31.

The Security World Software is supplied on the accompanying Security World for nShield installation media.

1.2 Additional documentation

You can find additional documentation in the **document** directory of the installation media, including the *nShield Edge and nShield Solo User Guide*, which describes how to use the Security World Software.

We strongly recommend that you read the release notes in the **re1ease** directory of your installation disc before you use the nShield Edge. These notes contain the latest information about your product.

See the User Guide for a glossary of terms.

1.2.1 Terminology

The nShield Edge is referred to as the *nShield Edge*, the *hardware security module*, or the *HSM*.

1.3 Typographical conventions

i The word **Note** indicates important supplemental 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

2 Safety and security

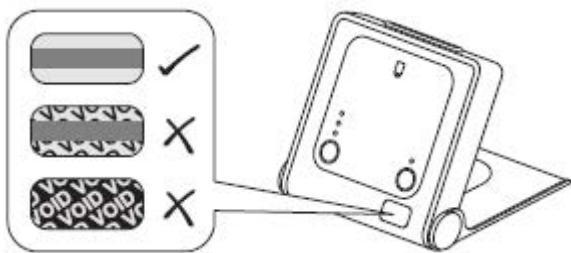


There are no user-serviceable parts inside the nShield Edge. Any attempt to dismantle the nShield Edge results in any remaining warranty cover, the maintenance and support agreement, or both being rendered void.

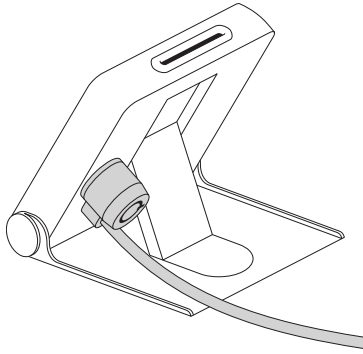
To help maintain security:

- Always inspect the USB cable and the nShield Edge before use, specifically the nCipher logo hologram in the tamper window shown below. (The nShield Edge Developer Edition does not have a hologram and tamper window.) If there are any signs of tampering, do not use the cable and the nShield Edge.

Figure 1. nCipher logo hologram in the tamper window



- Where possible, use the lock slot of the nShield Edge to secure it to a desk with a compatible lock (not supplied).

Figure 2. nShield Edge lock slot

- Never store or carry smart cards with the nShield Edge.
- Protect your pass phrase in line with your organization's security policy.

2.1 FIPS

There are a number of nShield Edge variants, some certified to different FIPS 140-2 levels. The FIPS rating is indicated on the label on the nShield Edge.

3 Regulatory notices

3.1 FCC class A notice

The nShield Solo and nShield Solo XC 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 user will be required to correct the interference at his own expense.

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

3.3 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 product, which is then disposed of in an environmentally safe manner. For further information or to arrange the safe disposal of your product, contact nCipher Support.

Avis juridiques

3.4 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.

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

3.6 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 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 nCipher Support.

Rechtliche Informationen

3.7 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 Wohngebieten kann möglicherweise störende Interferenzen verursachen. In einem solchen Fall muss der Nutzer die Interferenzen auf seine eigenen Kosten abstellen.

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

3.9 Informationen zu Recycling und Entsorgung

Gemäß der WEEE-Richtlinie (Waste Electrical and Electronic Equipment) wird zur Wiederverwertung von elektronischen Geräten ein Rücknahme- und Recyclingprogramm bereitgestellt. Im Rahmen dieses Programms können Sie veraltete oder nicht mehr genutzte nCipher 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 nCipher Support.

Notificaciones reglamentarias

3.10 Notificación clase A de la FCC

Este HSM nShield Solo cumple con la parte 15 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.

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

3.12 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 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.

4 Before you install the software

 Do not connect the nShield Edge to your computer before installing the Security World Software.

- Uninstall any older versions of Security World Software. See *Uninstalling existing software* on page 28.

4.1 Preparatory tasks before installing software

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

4.1.1 Windows environments

Adjust your computers power saving setting to prevent sleep mode.

4.1.1.1 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/>.

4.1.2 Unix Environments

4.1.2.1 Install operating environment patches

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

4.1.2.2 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.

4.1.3 All environments

4.1.3.1 Install Java with any necessary patches

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

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

We recommend 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 |

 You must have Java installed to use KeySafe.

4.1.3.2 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.

i You *must* install the **Hardware Support bundle**. If the **Hardware Support bundle** is not installed, your module cannot function.

i Ensure that the **Edge Monitor Controller** feature is selected during installation.

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

i 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.

4.2 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 | Use |
|------------|--------------|---|
| Hardserver | 9000 | Internal non-privileged connections from Java applications including KeySafe |
| Hardserver | 9001 | Internal privileged connections from Java applications including KeySafe |
| Hardserver | 9004 | Incoming impath connections from other hardservers, eg: <ul style="list-style-type: none"> • From a non-attended host machine to an attended host machine when using Remote Operator |

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 configuration file. See the *User Guide* for your module and operating system for more about configuration files.

5 Installing the software

This chapter describes how to install the Security World Software on the computer to which your nShield Edge will be connected.

After you have installed the software and connected an nShield Edge to your computer, 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.

 If you are planning to use an nToken with a client, this should be physically installed in the client before installing the Security World software, see *nToken Installation Guide*

5.1 Installing the Security World Software

5.2 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, including the **Edge Monitor Controller**, and then click **Next**. See *Components on Security World Software installation media (Windows and Unix) on page 31* 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
5. The installer advises you that the SNMP agent does not run by default. Click **Next** to continue.
 6. The installer advises you if you have an existing PKCS #11 installation. Click **Next** to continue.
 7. 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.
 8. Click **Finish** to complete the installation.
 9. Update your system environment **PATH** by inserting the sub-path **%NFAST_HOME%\bin**.

5.3 Installing Security World Software in a Linux environment

1. For **SOFTWARE to install**, select **List**, and then select all required file sets. See *Components on Security World Software installation media (Windows and Unix)* on page 31 for more about the component bundles and the additional software supplied on your installation media.

5.3.1 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, `11bc6_11`), `bundle` is the directory name of a given bundle (for example, `hwsp` or `ct1s`), and `file.tar` is the name of a `.tar` file within a bundle directory.

 Some directories contain more than one `.tar` file.

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

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

6. Log in to your normal account.
7. 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
```

6 Setting up the nShield Edge

6.1 Power saving options

- i** Do not use the power-saving features of your computer when the nShield Edge is connected. If your computer goes into standby or sleep mode, the hardserver restarts automatically.

If your computer has power saving features enabled, do the following:

1. For Windows installations: From the **Power Options** section of the Control Panel, select **Power Option > Change plan settings**.
2. For **Put the computer to sleep**, select **Never**
3. For Linux Installations: Set power options to never put computer to sleep.

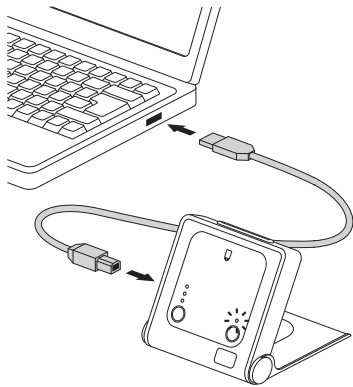
6.2 Connecting an nShield Edge

Do the following:

6.2.1 Windows

- Connect the nShield Edge to your computer, using the supplied USB cable.

Figure 3. Connecting the nShield Edge to your computer



If your operating system detects the nShield Edge automatically, allow it to finish.

On Windows installations a message appears, reporting that Windows is stopping and restarting the hardserver. This takes approximately 30 seconds. Do not click **Close**.

6.2.2 Linux

- Connect the nShield Edge to your computer, using the supplied USB cable.
- Open a terminal window and enter the following command `tail -f ${NFAST_HOME}/log/edgeHandler.log`.

- A message appears, reporting that Linux is stopping and restarting the hardserver. This takes approximately 30 seconds. Do not click **Close**.

When the hardserver has restarted, you are ready to use the nShield Edge with the Security World Software. See the *nShield Edge and nShield Solo User Guide* for more about creating a Security World and using the Security World Software. Creating a Security World involves putting the nShield Edge into Initialization (I) mode. See *Changing the mode on page 24* for more information.

6.3 Enabling optional features

The nShield Edge supports a range of optional features, which can be enabled with a certificate or Activator card that you order from nCipher. The features that are suitable for the nShield Edge are listed in the *Release Notes*.

To enable optional features, follow the instructions in the *nShield Edge and nShield Solo User Guide*, or follow the instructions supplied with the certificate or Activator card.

6.4 Disconnecting and reconnecting the nShield Edge

After use, you can disconnect the nShield Edge from the computer's USB port, and then reconnect it when you next need to use it. The hardserver stops and restarts automatically each time you disconnect or connect the nShield Edge.



Do not use the Windows Safely Remove Hardware system tray icon when disconnecting the nShield Edge. If you use this method, an error displays. Simply disconnect the nShield Edge from the computer's USB port.

Do not disconnect the nShield Edge or remove the smart card when data is being written to the inserted smart card.

6.5 Checking the installation

To check that the software and nShield Edge have been installed correctly:

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 HSM 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.

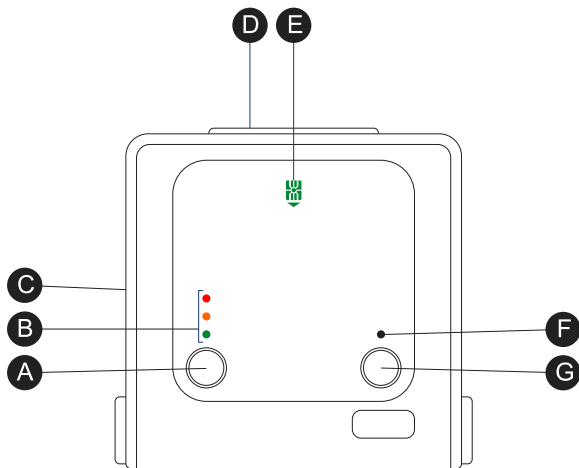
-  Ensure that the Windows power saving features are disabled. See [Power saving options](#) on page 20 for more information.

6.6 Using a Security World

See the *User Guide* for more about creating a Security World or loading an existing one.

7 Using the nShield Edge







Figure 4. The nShield Edge controls, card slot, and LEDs



Key:

| | |
|--------------------|---|
| A: Mode button | Selects a mode—the mode changes only when you press the Clear button. |
| B: Mode LEDs | Shows the current mode or selected mode. |
| C: B type USB port | For connecting the nShield Edge to the computer. |
| D: Card slot | For inserting the required smart card. |
| E: Card slot LED | Lights green when a smart card is inserted. |
| F: Status LED | Shows the status of the nShield Edge. |
| G: Clear button | Clears the memory of the nShield Edge and changes the selected mode. When using this button, press and hold it for a couple of seconds. |

7.1 Mode LEDs

| | | |
|---|----------------|------------------------------|
|  | Red | In Maintenance mode |
|  | Red flashing | Maintenance mode selected |
|  | Amber | In Initialization mode |
|  | Amber flashing | Initialization mode selected |
|  | Green | In Operational mode |
|  | Green flashing | Operational mode selected |

You generally use the nShield Edge in Operational (O) mode, but you must put it into Initialization (I) mode when creating the Security World.

7.2 Changing the mode





To change the mode:

1. Use the **Mode** button to highlight the required mode.
2. Within a few seconds, press and hold the **Clear** button for a couple of seconds.

If the mode changes, the new mode's LED stops flashing and remains lit. The Status LED might flash irregularly for a few seconds and then flashes regularly when the nShield Edge is ready.

Otherwise, the nShield Edge remains in the current mode, with the appropriate mode LED lit.

7.3 Status LED

| | | |
|---|------------------|---------------------------------------|
|  | Long blue flash | In Operational mode |
|  | Short blue flash | In Maintenance or Initialization mode |
|  | Irregular flash | Changing mode or processing data |
|  | Off | No power |

If the Status LED flashes irregularly and the nShield Edge is unresponsive for more than a few minutes, see *Troubleshooting*.

8 Troubleshooting

If the nShield Edge does not function as expected, check the symptoms against the following conditions and try the suggested action. If these actions do not solve your problem, contact nCipher Support.

8.1 None of the LEDs are lit

The nShield Edge is not receiving power. Check that the USB cable is undamaged and connected to the nShield Edge and computer. Try another USB port on the computer.

8.2 The Mode LED is amber or red

The nShield Edge is not in the Operational (O) mode. Press the **Mode** button to select the Operational mode, and then press and hold the **Clear** button for a couple of seconds. Wait a few seconds before using the nShield Edge.

8.3 The Status LED is flashing irregularly and the nShield Edge is unresponsive for more than a few minutes

The nShield Edge has encountered an error. Disconnect the nShield Edge, wait a few seconds, and then reconnect it.

8.4 The Security World Software does not detect the connected nShield Edge

Disconnect the nShield Edge, wait a few seconds, and then reconnect it.

Run the **enquiry** command. If the command output says that the module is not found, restart the hardware server by following the instructions in the *nShield Edge and nShield Solo User Guide*.

8.5 Upgrading the firmware

If you are instructed to upgrade firmware of the nShield Edge, see the *nShield Edge and nShield Solo User Guide* for instructions.

8.5.1 Contacting nCipher Support

To obtain support for your product, visit: <https://help.ncipher.com>.

9 nShield Edge Windows compatibility issues and considerations

9.1 nShield Edge very slow in VMware virtual machine

In Windows installations nShield Edge can be very slow when used with a virtual machine under VMware (Workstation or Player) leading to the COM port timing out and errors in the Event log.

The problem does not happen in all installations and is not consistent on specific hardware platforms.

The work-around for the problem involves using the USB Serial driver on the Host rather than on the Guest, and mapping a serial port on the Guest to it (details below)

To apply the work-around to use the USB to serial driver on the Host rather than on the Guest, do the following:

1. With the Guest running, use the VMware Workstation/Player menu to disconnect the nShield Edge from the Guest and reconnect it to the Host. Now shut down the Guest.
2. Verify that the USB Serial Port now shows under Ports (COM & LPT) in Device Manager on the Host. On recent versions of Windows, the driver will be installed automatically or can be found via Window Update. If you are unable to find the drivers you may need to install the Security World Software on the Host. If you do so, make sure to stop and disable the nFast Server and nFast Edge services on the Host, so they do not prevent the Guest from using of the unit. Make a note of the COM port number of the port.
3. Edit the settings of the Virtual machine in Workstation/Player. Disable the setting to automatically connect to new USB devices to make sure the Guest will not connect to the nShield Edge directly again. Add a serial port to the VM, specifying to use a physical serial port, on the host, and selecting the USB serial port from the previous step. Save the settings.
4. Start the Guest. Open the config file in a text editor - it is a plain text file named config (no extension), located in %NFAST_KMDATA%\config. In the section [server_startup] add a line: serial_dtp devices=COM2 specifying the COM port number of the new serial port in the VM. Make sure this is the only line with serial_dtp devices in the section. Save the file, and restart the nFast Server service to make the new configuration active.

You can now use the nShield Edge in the Guest without excessive time out errors.

10 Dimensions and operating conditions

| | |
|---|-------------------------------|
| Dimensions (with stand closed) | 120 (w) x 118 (h) x 27 (d) mm |
| Weight | 340g |
| Powered by USB host device | 5V, 700mW |
| Operating temperature | 5 – 45 °C |
| Storage temperature | -40 – 70 °C |
| Operating and storage relative humidity | 10 – 85% non-condensing |






10.1 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.

Appendix A Uninstalling existing software

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

-  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.
-  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.
-  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.
-  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.
-  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.

A.1 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.

A.2 Uninstalling Unix software

A.2.1 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
```



Deleting all the files and subdirectories in `/opt/nfast` also deletes the `/opt/nfast/kmdata` directory. To be able to restore an existing Security 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.



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 18](#).

nCipher supply the hardware server 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.

B.1 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:

B.1.1 Component bundles

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

B.1.2 Individual components

| Unix Package | Description (Windows and Unix) |
|--------------|---|
| | nCipher CAPI-NG providers and tools - Windows only |
| hwcrhk | Crypto Hardware Interface (CHIL) plugin |
| jcecspp | 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 |

B.2 CipherTools installation media

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

B.2.1 Component bundles

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

B.2.2 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 |
| jcecs | 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 |

B.3 CodeSafe installation media

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

B.3.1 Component bundles

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

B.3.2 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 |
| jcecsf | 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 |

B.4 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.

B.4.1 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.

B.4.1.1 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 |

B.4.1.2 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) |
|---------------------|--|
| <code>convrt</code> | Command line key conversions |
| <code>nftcl</code> | Command line key management (Tcl) |
| <code>nftcl</code> | Command line key generation and import |
| <code>nfuser</code> | Low level utilities and test programs |
| <code>nfuser</code> | Command line remote server management |
| <code>opensl</code> | nftcl certificate generation utility |
| <code>sworld</code> | Command line key management (C) |
| <code>tclsrc</code> | Tcl run time |
| <code>tclstf</code> | Small Tcl utilities |
| <code>nftcl</code> | Command line key generation and import |
| <code>tct2</code> | Trusted Code Tool 2 command-line utility |
| <code>pysrc</code> | Python source for developers |
| <code>nfpv</code> | |

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



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.

B.4.1.3 Java Support (including KeySafe)

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

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

B.4.1.4 Remote Administration Service

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

B.4.1.5 Remote Administration Client

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

B.4.1.6 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.

B.4.2 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.

B.4.2.1 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 |
| emvsp | 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 |
| nfpyp | nFPython header files |

B.4.2.2 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 |
| ssl-lib | Codesafe-SSL hostside code |
| ssl-lib | Codesafe-SSL moduleside code |
| pysrc | Python source for developers |
| nfpyp | nFPython header files |
| nfpyp | Libs and headers for codesafe/python |

B.4.2.3 Java Developer

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

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

B.5 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 nC4nn2 or Bn1 nnn, install the **Prebuilt arm-gcc for Codesafe/C** component.
- If your module has a part code of the form nC4nn3, 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.

B.5.1 KeySafe

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

B.5.2 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**

B.5.3 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>.

B.6 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.

-  Security World Software supports OpenSSL 1.0.1g and later.

B.7 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.

B.8 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.