nShield Security World

nShield nToken v12.81 Install Guide

12 July 2024

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
    1.1. About this guide . . . 1
    1.2. Model numbers . . . 1
    1.3. Additional documentation . . . 1
2. Hardware security modules . . . 3
    2.1. Power requirements . . . 3
    2.2. Handling modules . . . 3
    2.3. Environmental requirements . . . 3
    2.4. Module operational temperature and humidity specifications . . . 4
    2.5. Cooling requirements . . . 5
    2.6. Physical location considerations . . . 5
3. Regulatory notices . . . 7
    3.1. FCC class A notice . . . 7
    3.2. Canadian certification - CAN ICES-3 (A)/NMB- 3(A) . . . 7
    3.3. Recycling and disposal information . . . 7
4. Before installing the module . . . 8
    4.1. Module pre-installation steps . . . 8
    4.2. Fitting a module bracket . . . 8
5. Installing the module . . . 9
    5.1. After installing the module . . . 9
6. Before you install the software . . . 10
    6.1. Preparatory tasks before installing software . . . 10
        6.1.1. Windows . . . 10
        6.1.2. Linux . . . 10
        6.1.3. All environments . . . 11
    6.2. Firewall settings . . . 12
7. Installing the software . . . 14
    7.1. Installing the Security World Software on Windows . . . 14
    7.2. Installing the Security World Software on Linux . . . 15
8. Status indicators . . . 18
    8.1. Status LED . . . 18
    8.2. Solo . . . 18
9. Configuring and checking the installation . . . 20
    9.1. Adding the client to the nShield Connect . . . 20
    9.2. Checking the installation . . . 21
    9.3. Using a Security World . . . 22
10. Uninstalling existing software . . . 23

10.1. Uninstalling the Security World Software on Windows . . . 24
10.2. Uninstalling the Security World Software on Linux . . . 24
11. Software packages on the Security World installation media . . . 26
11.1. Security World installation media . . . 26
11.1.1. Component bundles . . . 26
11.2. Components required for particular functionality . . . 27
11.2.1. KeySafe . . . 27
11.2.2. Microsoft CAPI CSP and Microsoft Cryptography API: Next Generation (CNG) . . . 27
11.3. nCipherKM JCA/JCE cryptographic service provider . . . 28
11.4. SNMP monitoring agent . . . 28

1. Introduction

The Entrust 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.

1.1. About this guide

This guide includes:

- Installing the nToken. See Installing the module.
- Installing the Security World Software. See Installing the software.
- A description of the module status indicators. See Status indicators.
- Instructions about removing existing software. See Uninstalling existing software.

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

1.2. Model numbers

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

Model number	Used for
xC2021E-000 xC2023E-000	nToken PCIe

1.3. Additional documentation

You can find additional documentation in the `documentation` directory of the installation media for your product. For information about using the software, see the *nShield Connect User Guide*. Entrust strongly recommends that you read the release notes at

https://trustedcare.entrust.com/. These notes contain the latest information about your product.

2. Hardware security modules

2.1. Power requirements

Module	Maximum power
Solo	9.9W
Solo XC	24W
nShield 5s	25W

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

The module is intended for installation into a certified personal computer, server, or similar equipment.

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

2.2. Handling modules

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

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

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

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

2.3. 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.

2.4. Module operational temperature and humidity specifications

The Solo modules operate within the following environmental conditions.

Solo 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 Solo XC module operates within the following environmental conditions.

Solo XC environmental conditions	Operating range		Comments
	Min.	Max.	
Ambient operating temperature	5°C	55°C	-
Storage temperature	-5°C	60°C	-
Transportation temperature	-40°C	70°C	-
Operating humidity	5%	85%	Relative. Non-condensing at 30°C
Storage humidity	5%	93%	Relative. Non-condensing at 30°C
Transportation humidity	5%	93%	Relative. Non-condensing at 30°C

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

nShield 5s environmental conditions	Operating range		Comments
	Min.	Max.	

Ambient operating temperature	5°C	55°C	-
Storage temperature	-5°C	60°C	-
Transportation temperature	-40°C	70°C	-
Operating humidity	5%	85%	Relative. Non-condensing at 30°C
Storage humidity	5%	93%	Relative. Non-condensing at 30°C
Transportation humidity	5%	93%	Relative. Non-condensing at 30°C

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

2.5. 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:

Solo, Solo XC

Stops operating and displays the `SOS-T` error message on the Status LED.

nShield 5s

Stops operating and displays an error message on the Status LED.

See Status indicators.

2.6. Physical location considerations

Entrust 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.

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 users will be required to correct the interference at their own expense.

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

3.3. Recycling and disposal information

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

4. Before installing the module

4.1. Module pre-installation steps

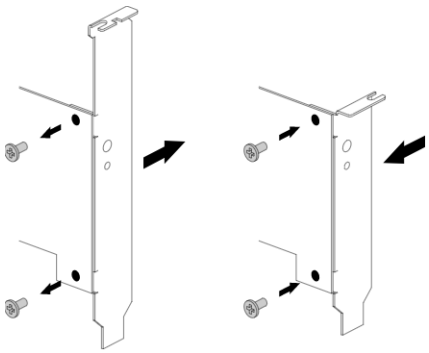
Check the module to ensure that there is no sign of damage or tampering:

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

4.2. Fitting a module bracket

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

Do not touch the connector pins, or the exposed area of the module without taking ESD pre cautions.



To fit the bracket to the module:

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

5. Installing the module

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

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

   Minimum requirement:

nToken	1 PCIe x1 slot

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

5.1. After installing the module

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.

6. Before you install the software

- Uninstall any older versions of Security World Software. See Uninstalling existing software.

6.1. Preparatory tasks before installing software

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

6.1.1. Windows

6.1.1.1. Power saving options

Adjust your computers power saving setting to prevent sleep mode.

6.1.1.2. Install Microsoft security updates

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

6.1.2. Linux

6.1.2.1. Install operating environment patches

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

6.1.2.2. Users and groups

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

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

group, using `/opt/nfast` as the home directory.

6.1.3. All environments

6.1.3.1. Install Java with any necessary patches

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

- Java7 (or Java 1.7x)
- Java8 (or Java 1.8x)
- Java11.

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

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

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

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

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

You must have Java installed to use KeySafe.

6.1.3.2. Identify software components to be installed

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

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

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

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

On Windows, the **nShield Hardware Support bundle** and the **nShield Core Tools bundle** are mandatory, and are always installed.

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

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

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

- `generatekey`
- Low level utilities
- Test programs

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

6.2. Firewall settings

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

Component	Default Port	Use
Hardserver	9000	Internal non-privileged connections from Java applications including KeySafe
Hardserver	9001	Internal privileged connections from Java applications including KeySafe

Component	Default Port	Use
Hardserver in nShield Connect	9004	Incoming impath connections from client machines.

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.

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*.

7.1. Installing the Security World Software on Windows

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

For a regular installation:

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.msi` manually when prompted.
3. Follow the onscreen instructions. Accept the license terms. Select **Next** to continue.
4. Specify the installation directory. Select **Next** to continue.
5. Select all the components required for installation, and then select **Install**. All components will be selected by default. Unselect via dropdown menu for individual component that you do not wish to install. **nShield Hardware Support** and **Core Tools** are necessary to install the Security World Software. See Software packages on the Security World installation media for more about the component bundles and the additional software supplied on your installation media.

   The selected components are installed in the installation directory chosen above. The installer creates links to the following nShield Cryptographic Service Provider (CSP) setup wizards as well as remote management tools under **Start** > **All Programs** > **nCipher**:

   - If **nShield CSPs (CAPI, CNG)** was selected: **32bit CSP install wizard**, which sets up CSPs for 32-bit applications
   - If **nShield CSPs (CAPI, CNG)** was selected: **64bit CSP install wizard**, which sets up CSPs for 64-bit applications

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

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

6. Select **Finish** to complete the installation.
7. The following global variables are set upon install:
   - `%NFAST_CERTDIR%`
   - `%NFAST_HOME%`
   - `%NFAST_KMDATA%`
   - `%NFAST_LOGDIR%`

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

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

7.2. Installing the Security World Software on Linux

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/<file>.tar.gz
   ```

   In this command, `ver` is the architecture of the operating system (for example, i386 or amd64), and `file.tar` is the name of a `.tar.gz` file for that component.

5. To use an nShield module with your Linux system, you must build a kernel driver.

Entrust supplies the source to the (nfp) and a makefile for building the driver as a loadable module.

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

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

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

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

Solo and Solo XC

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

nShield 5s

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

b. Make the driver by running the command:

```
# make
```

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

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

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

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

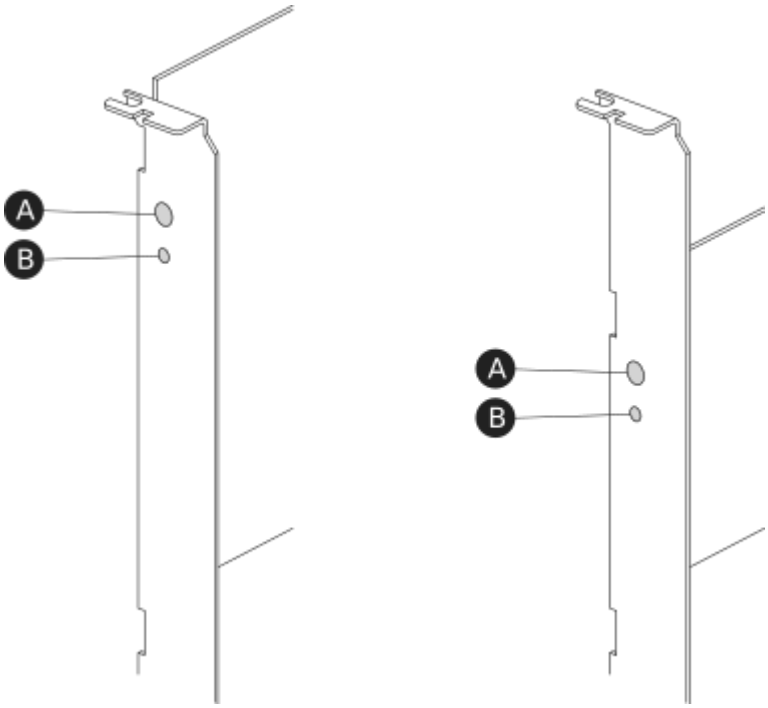
If you use the Bourne shell, add these lines to your system or personal profile:

```
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
```

8. Status indicators



Label	Description
A	Status LED
B	Recessed clear button

8.1. Status LED

8.2. Solo

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 nShield Solo module is accepting commands. The more frequently the Status LED blinks off, the greater the load on the module.

Status LED	Description
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*.

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.

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

9.1. Adding the client to the nShield Connect

When the client is added to the nShield Connect, the client must use the nToken to commu nicate 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 **Sys tem > System configuration > Client configuration > New client**.
2. Enter the IP address and netmask of the first client, and press the right-hand naviga- tion 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 avail able 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 Linux.
Priv. on any ports	Privileged connections are allowed on all ports.

You need a privileged connection to perform module administra- tion tasks (for example, to create a Security World). If you are not going to perform module administration tasks, Entrust recom- mends that you allow only unprivileged connections. For more infor mation, see the *nShield Connect User Guide*.

When you have selected the type of connection, press the right-hand navigation button.

4. 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.
5. 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
      ```

   b. 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.
6. 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 reported the
   software key hash:

   691be427bb125f387686
   38a18bfd2eab75623320

   Is this EXACTLY right?

   CANCEL    CONFIRM
   ```

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

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

9.2. 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
   ```

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 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.

Under Windows 7 and Windows 2008 R2, ensure that the power saving features are disabled. See Installing the module. 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.

9.3. Using a Security World

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

10. Uninstalling existing software

Entrust 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 user created components, key data, or Security World data.

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

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.

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 on Linux.

If you are downgrading a software authenticated client to a Security World Software earlier than version 12.60, the client will need to be re-enrolled as software-based authentication is not supported. See the *Configuring the nShield Connect to use the client* section in the _nShield Connect User Guide_for more information.

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

10.1. Uninstalling the Security World Software on Windows

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

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

10.2. Uninstalling the Security World Software on Linux

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

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

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

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

   ```
   $ su -
   ```

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

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

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

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

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

nShield 5s only

> Deleting all the files and subdirectories in `/opt/nfast` also deletes the `/opt/nfast/services` directory. This will make it impossible to communicate with the HSM after re-installation unless it is first fac tory stated. The recommended procedure is to reset the HSM to factory state using `hsmadmin factorystate` before uninstalling the software. If this is not possible, or has not been done, then reset the HSM to factory state by booting into recovery mode.

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.

11. Software packages on the Security World installation media

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

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

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

11.1. Security World installation media

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

11.1.1. Component bundles

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

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

11.2. Components required for particular functionality

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

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

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

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

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

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

11.2.1. KeySafe

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

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

If you require the Microsoft CAPI CSP, you must install the nShield CSPs (CAPI, CNG) com-

ponent.

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

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

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

11.3. nCipherKM JCA/JCE cryptographic service provider

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

- The nShield Java bundle

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

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

11.4. SNMP monitoring agent

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

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

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

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