



ENTRUST

nShield Security World

nShield Security World Software v13.6.5 Installation Guide

05 November 2024

Table of Contents

1. Before you install the software	2
1.1. Preparatory tasks before installing software	2
1.1.1. Windows	2
1.1.2. Linux	3
1.1.3. All environments	5
1.2. Firewall settings	7
2. Install the Security World software	9
2.1. Installing the Security World Software on Windows	9
2.1.1. Additional steps for nShield 5s	11
2.2. Install the Security World software on Linux	12
2.3. After installing the software	15
3. Using silent installations	17
3.1. Installing using the silent install functionality	17
3.2. Uninstalling using the silent install functionality	18
4. Problems during installation and commissioning	19
4.1. PCIe HSMs	19
5. Uninstalling Security World Software	20
5.1. Uninstalling the Security World software on Windows	20
5.1.1. Removal of Security World data	21
5.2. Uninstalling the Security World software on Linux	21
6. System upgrade	23
6.1. Software and firmware compatibility	23
6.2. System upgrade procedure	23
6.3. Upgrade software	24
6.3.1. Before upgrading software	24
6.3.2. Reinstall Security World software	25
6.3.3. After upgrading software	25
6.4. Upgrade firmware	25
7. Software packages on the installation media	26
7.1. Security World installation media	26

Chapter Preface

This guide provides installation instructions to help you install the Security World software on the computer, client, or RFS associates with your nShield HSM.

Ensure that you follow the preparation and installation instructions relevant for your HSM.

1. Before you install the software

This guide covers the following HSMs:

- nShield Solo
- nShield Solo XC
- nShield 5s
- nShield Connect
- nShield 5c
- nShield Edge

Before you install the Security World software:

- **(PCIe HSMs only)** Install the module. See [Install a PCIe HSM](#).
- Uninstall any older versions of Security World Software. See [Uninstalling Security World Software](#)
- If the nShield Remote Administration Client is installed on the machine, remove it. You will also have to re-install it after you installed the new Security World software version. See [Remote Administration v13.6.5 User Guide](#).
- Complete the [preparatory tasks](#).

1.1. Preparatory tasks before installing software

1.1.1. Windows

1.1.1.1. Turn off sleep mode

Adjust your computer's power saving setting to prevent sleep mode.

1.1.1.2. 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/>.

1.1.1.3. **(PCIe HSMs only)** Add %NFAST_HOME%\bin\ to the PATH environment variable

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

If you cannot change **PATH**, you will have to enclose all file names and paths that use variable between double quotation marks (" "). For example:

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

1.1.2. Linux

1.1.2.1. Install operating environment patches

Make sure that you have installed:

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

See the documentation supplied with your operating environment for information.

1.1.2.2. 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.



(USB HSMs only) The **nfast** user must also be a member of the **dialout** group. **dialout** grants access to the serial ports, including those that the nShield Edge uses (**/dev/ttyUSB***).

For example, on Linux, run:

```
useradd -a -G dialout nfast
```

- 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.

1.1.2.3. (nShield 5s only) Network configuration

The nShield 5s appears to the host operating system as a network interface.

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

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

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

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

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

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

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

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

Outbound SSH traffic on TCP ports:

- 2201
- 2202
- 2203
- 2204
- 2206

1.1.3. All environments

1.1.3.1. 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.

1.1.3.2. 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.

Network-attached HSMs

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

PCIe HSMs

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

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

On Linux, you *must* install the **hwsp** component and, for **nShield 5s HSMs** the **nshield5_net** component.

USB HSMs

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

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.

Network-attached and PCIe HSMs only

You need to install the Remote Administration Service component if you require remote administration functionality. See [\[software-install:preinstall-sw:::prep\]](#) and [Remote Administration v13.6.5 User Guide](#) for more about the Remote Administration Service.

Always install all the nShield components you need in a single installation process to avoid subsequent issues should you wish to uninstall. You should not, for example,

install the Remote Administration Service from the Security World installation media, then later install the Remote Administration Client from the client installation media.

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

1.2. Firewall settings

When setting up your firewall, you should ensure that the port settings are compatible with the HSMs and allow access to the system components you are using.

The following table identifies the ports used by the nShield system components. All listed ports are the default setting. Other ports may be defined during system configuration, according to the requirements of your organization.

Component	Default Port	Protocol	Use
Hardserver	9000	TCP	Internal non-privileged connections from Java applications including KeySafe
Hardserver	9001	TCP	Internal privileged connections from Java applications including KeySafe
Hardserver	9004	TCP	Incoming impath connections from other hardservers, for example: <ul style="list-style-type: none"> • From an HSM to the Remote File System (RFS) (network-attached HSMs). • From a cooperating client to the RFS it is configured to access (PCIe HSMs). • From a non-attended host machine or HSM to an attended host machine when using Remote Operator.
Hardserver in the HSM (network-attached HSMs only)	9004	TCP	Incoming impath connections from client machines
Remote Administration Service	9005	TCP	Incoming connections from Remote Administration Clients
Audit Logging syslog	514	UDP	If you plan to use the Audit Logging facility with remote syslog or SIEM applications, you need to allow outgoing connections to the configured UDP port

Component	Default Port	Protocol	Use
mDNS (nShield 5s only)	5353	UDP	Send out mDNS Service Discovery requests and receive responses

If you are setting up an RFS or exporting a slot for Remote Operator functionality (**network-attached HSMs**) or using an nShield Edge as a Remote Operator slot for an HSM located elsewhere (**PCIe and USB HSMs**), 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 see [HSM and client configuration files](#) (network-attached HSMs) or [Hardserver configuration files](#) (PCIe and USB HSMs) for more about configuration files. Similarly, if you are setting up the Remote Administration Service you need to open port 9005.

2. Install the Security World 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.

2.1. Installing the Security World Software on Windows

For information about configuring silent installations and uninstallations on Windows, see [Using silent installations](#).

For a regular installation:



(**nShield 5s only**) Installing Security World software on Windows via Remote Desktop Connection can result in a brief loss of RDP connection. If this happens, it will happen during the **Status:** part of the installation, towards the end. When the session reconnects, the installation carries on until completion.

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



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

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

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

See [Software packages on the installation media](#) for more about the component

bundles and the additional software supplied on your installation media.

8. Select **Install**.

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

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

If selected, the SNMP agent will be installed, but will not be added to the **Services** area in **Control Panel > Administrative Tools** of the target Windows machine. If you wish to install the SNMP agent as a service, consult the [nShield SNMP Monitor v13.6.5 Install and User guide](#).



(PCIe HSMs only) Do not run any CSP installation wizard before installing the module hardware.

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

The following global variables are set upon install:

- **%NFAST_CERTDIR%**
- **%NFAST_HOME%**
- **%NFAST_KMDATA%**
- **%NFAST_LOGDIR%**
- **%NFAST_SERVICES_HOME%** (**nShield 5s only**)

10. Add **C:\Program Files\nCipher\nfast\bin** to the Windows system path.

11. (**nShield 5s only**) If you are using an nShield 5s, complete the [additional steps for nShield 5s](#).

12. **(PCIe HSMs only)** If you are using a PCIe HSM, you might need to update the power saving settings:
 - a. In **Windows Device Manager > Security Accelerator (nShield Solo)** or **Windows Device Manager > Network adapters (nShield 5s)**, select the appropriate module.
 - b. Under **Properties > Power Management**, deselect **Allow the computer to turn off this device to save power**.

2.1.1. Additional steps for nShield 5s

1. Stop the nFast Server service.
2. The nShield installer creates and enables an inbound rule called **nShield 5s mDNS** to allow UDP port 5353 for any program. This enables the discovery of nShield 5s modules. If enrollment fails to find any modules in the following step, check that this firewall rule is present and enabled; if it does not exist, create it manually and retry enrollment.
3. Set up the secure communication channels between the host PC and the HSM:

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



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

From firmware versions 13.5 onwards, the secure communication channels between the host PC and the HSM are protected by internally generated certificates. The **hsmadmin enroll** command automatically validates certificates as part of the enrollment process and produces a warning if it fails to find a certificate for any service. This warning is expected if the HSM:

- is in recovery mode
- is running a firmware version prior to 13.5
- has been upgraded to a firmware version of 13.5 or later but has not performed a factory state operation since the upgrade.

If you receive this warning in any other circumstance you should contact Entrust support.

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

2.2. Install the Security World software on Linux

1. Sign in as a user with `root` privileges.
2. Mount the DVD/ISO image.
3. Open a terminal window, and change to the `root` directory.
4. Extract the required files if you are using `.tar` or install the `rpm` packages if you are using the `rpm` utility.

<disc-name>	Name of the mount point of the installation media
<ver>	Architecture of the operating system, for example, <code>i386</code> or <code>amd64</code>
<file.tar>	Name of the <code>.tar.gz</code> file for the component
<file.rpm>	Name of the <code>.rpm</code> file for the component

From `.tar`

Install all the software bundles by running `tar`:

```
tar -xf <disc-name>/linux/<ver>/<file>.tar.gz
```

From `.rpm`

- a. Import the public key in `<disc-name>/linux-rpms/<ver>/pubkey.asc` into `rpm`:

```
rpm --import <disc-name>/linux-rpms/<ver>/pubkey.asc
```

- b. Verify that the `.rpm` files are signed by Entrust:

```
rpm --checksig <disc-name>/linux-rpms/<ver>/<file>.rpm
```

- c. Install all the software bundles by running `rpm`.

If a subset of the packages is already installed and you have to install more packages, uninstall the installed packages, then install all the `.rpm` packages that you need from fresh. See [Uninstalling Security World Software](#) for more information.

You must install the `hwsp` package first. If you have to re-install `hwsp`, uninstall it last, then re-install it first.

```
rpm -i disc-name/linux-rpms/<ver>/<file>.rpm
```

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. **(PCIe HSMs only)** Change directory to the nShield PCI driver directory by running the command:

nShield Solo or Solo XC

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

nShield 5s

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

- b. (**nShield Solo and Solo XC only**) Configure the source by running the command:

```
./configure
```

- c. 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
```

(**nShield 5s only**) The install script will automatically run the `hsmadmin enroll` command. From firmware versions 13.5 onwards the secure communication channels between the host PC and the HSM are protected by internally generated certificates. The `hsmadmin enroll` command automatically validates certificates as part of the enrollment process and produces a warning if it fails to find a certificate for any service. This warning is expected if the HSM:

- is in recovery mode
- is running a firmware version prior to 13.5
- has been upgraded to a firmware version of 13.5 or later but has not performed a factory state operation since the upgrade.

If you receive this warning in any other circumstance you should contact Entrust support.

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

Bourne shell

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

C shell

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



(**nShield 5s only**) Entrust recommends that you take a backup of your

`sshadmin` key.

For example, you could use `hsmadmin keys backup /root/.ssh/id_nshield5_sshadmin` for backups that will be restored to the same machine. If the path `/root/.ssh/id_nshield5_sshadmin` is used, and the `sshadmin` key is missing from the usual installed location under `/opt/nfast`, then that key will be used automatically when running the nShield install script.

Note that this key will not be usable on another machine or if the OS is re-installed as it has protections tied to the local machine. For backups that may be restored to a different machine or re-installed OS, use `hsmadmin keys backup --passphrase /path/to/backup_key` to protect the key with a user-supplied passphrase (replacing `/path/to/backup_key` with the actual path to where the backup key should be written).

2.3. After installing the software

After you have successfully installed the Security World Software, complete the following steps to finish preparing your HSM for use:

1. Ensure that your public firewall is set up correctly.
See [Before you install the software](#).
2. **nShield 5s:** If the SSH keys have not been set up, create the communication path between the host machine and the HSM, as described in [Set up communication between host and module \(nShield 5s HSMs\)](#).



If you followed all the steps in the installation instructions when installing the software, this should already be set up.

3. **Network-attached HSMs:** Perform the necessary basic HSM-client configuration tasks, as described in [Basic HSM and remote file system \(RFS\) configuration](#).
4. **PCIe and USB HSMs:** If necessary, perform additional software and HSM configuration tasks, as described in [Client software and module configuration: PCIe and USB HSMs](#):
 - Set up client configuration, as described in [Client cooperation](#)
 - Set nShield specific environment variables, as described in [Setting environment variables](#).
 - Configure logging and debugging parameters, as described in [Logging and debugging](#)

- Configure Audit Logging, as described in [Configuring audit logging](#)
 - Configure Java support for KeySafe, as described in [Configuring Java support for KeySafe](#)
 - Configure the hardserver, as described in [Configuring the hardserver](#)
5. Create and configure a Security World, as described in [Create a new Security World](#).
 6. Create an OCS, as described in [Creating Operator Card Sets \(OCSs\)](#).
 7. **Network-attached HSMs:** Complete additional necessary HSM-client configuration tasks:
 - a. To configure the unit so that it works with the client machine, see [Configuring the nShield HSM to use the client](#).
 - b. To configure client computers so that they work with the unit, see [Configuring client computers to use the nShield HSM](#).



For this release, you must generate a new client configuration file to take advantage of new functionality. To generate a new client configuration file, back up your existing configuration file and run `cfg-mkdefault`. This generates a template for the configuration file into which you can copy the settings from your old configuration file.

- c. To enable the TCP sockets for Java applications (including KeySafe), run the command:

```
config-serverstartup -sp
```

For more information, see [Client configuration utilities](#).

When all additional HSM configuration tasks are completed, you can:

1. Stop and then restart the hardserver, as described in [Stopping and restarting the hardserver](#).
2. Test the installation and configuration.

3. Using silent installations

This guide describes how to use the command line for software installation and uninstallation for automation.

When you follow the standard installation instructions for Security World Software, the `setup.msi` installer runs automatically when you place the Security World Software installation media in the optical disc drive. You then follow the on-screen instructions from the installer to configure your installation.

However, if you run the `setup.msi` installer from the command line, you have the option to define the components you want to install via the Windows command prompt. This allows your installations to run 'silently', without the need for further interaction with the installer.

3.1. Installing using the silent install functionality

The Windows Installer (MSI) has the ability to install software without user interaction. This is useful for automation purposes.

Before starting, please ensure that:

- Any previously installed Security World Software is uninstalled
- If the directory `C:\Program Files\nCipher` exists, it is deleted
- If the directory `C:\ProgramData\nCipher` exists, it is renamed or deleted

To install the nShield Software using the silent install functionality:

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. If the installer runs automatically, quit the installer.
3. Open a Command Prompt, and run the command:

```
msiexec /i <PATH_TO_MSI> /quiet /forcerestart
```

This installs the nShield Security Software to the default installation directory, `%PROGRAMFILES%\nCipher\nfast\`, and restarts the machine.

To generate a verbose install log, add `/l*v <path-to-file.txt>` to the command after the `/quiet` argument. For example:

```
msiexec /i E:\setup.msi /quiet /l*v C:\users\USER_NAME\installLog.txt /forcerestart
```

This creates a log file in the specified directory.

3.2. Uninstalling using the silent install functionality

To uninstall the nShield Security Software using the silent uninstall functionality:

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. If the installer runs automatically, quit the installer.
3. Open a Command Prompt, and run the command:

```
msiexec /x <PATH_TO_MSI> /quiet /forcerestart
```

This uninstalls the nShield Security Software packages and restarts the machine.

To generate a verbose uninstall log, add `/l*v <path-to-file.txt>` to the command after the `/quiet` argument. For example:

```
msiexec /x E:\setup.msi /quiet /l*v C:\users\USER_NAME\uninstallLog.txt /forcerestart
```

This creates a log file in the specified directory.

4. Problems during installation and commissioning

4.1. PCIe HSMs

If problems are encountered when installing or commissioning an nShield HSM which prevent services from starting it will not be possible to use any of the debugging and logging tools described in [Checking the installation](#)

In this situation the command `hsm diagnose` may help identify network and hardware issues that are preventing the system from starting.

This command requires `root` privileges on Linux and the privileges of the built-in local Administrators group on Windows.

```
hsm diagnose
```

The command takes no parameters:

When the command is executed it will run a series of diagnostics tests and store the results in a file on the client PC. The information in the file is primarily intended for use by Entrust Support but you may be able to use the information to diagnose the issue yourself. If you are unable to do so, contact Entrust Support and send them a copy of the results file.

5. Uninstalling Security World Software

This section describes how to uninstall Security World software.

Entrust recommends that you only uninstall the Security World software in the following circumstances:

- You are certain it is no longer required.
- You intend to upgrade it.

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.

In Linux environments, it is also not possible to have more than one Security World software installation on the same computer.

Entrust therefore recommends that, when you are upgrading, any older versions of software are uninstalled and deleted.

The automated Security World software installers do not delete user created components, key data, or Security World data. However:

- On Linux, a manual installation using **.tar** files **does** overwrite existing data and directories.
- On Windows, 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.



nShield 5s

Make sure you have completed the steps described in [before upgrading software](#) before you uninstall any software.

5.1. Uninstalling the Security World software on Windows

This procedure requires the privileges of the built-in local Administrators group.

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.**

3. If the file `nCipherKM.jar` is present, it is located in the extensions folder of your local Java Virtual Machine. The uninstall process may not delete this file and you have to remove it manually.

5.1.1. Removal of Security World data

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

If you wish to completely uninstall the Security World, including any data created during its operation, including key data, navigate to the installation directory and delete the files in the `%NFAST_KMDATA%` folder.



Do not remove Security World data as part of an upgrade procedure. Only remove Security World data if you wish to do a complete uninstallation.

5.2. Uninstalling the Security World software on Linux

This procedure requires `root` privileges.

1. To remove drivers, install fragments, and scripts and to stop services, run the command:

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

2. If you have installed packages with `rpm`, you must also remove them with `rpm`:
 - a. Check which `rpm` packages are installed on the system:

```
rpm -qa nShield*
```

Example output:

```
For example, the output of this command on a test system looks as so:  
nShield-hwsp-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64  
nShield-csdref-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64  
nShield-csd-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64  
nShield-ctd-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64  
nShield-ctls-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64  
nShield-devref-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64  
nShield-javasp-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64  
nShield-jd-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64  
nShield-ncsnmp-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64  
nShield-raserv-237.a1f2123456789ffffffffd1d0d996f12272a98928-13.4.2.x86_64
```

- b. Follow the package list from the output **bottom up** to uninstall the packages one by one:

```
rpm -e <full-package-name>
```

For example:

```
rpm -e nShield-hwsp-237.a1f2123456789fffffffffd1d0d996f12272a98928-13.4.2.x86_64
```

From the output above, uninstall **raserv** first and uninstall **hwsp** last.



Files that were created after an **rpm** was installed are not deleted.

3. Delete all the files, including those in subdirectories, from **/opt/nfast** and **/dev/nfast/**:



The following commands delete both software and data. If you are uninstalling as part of an upgrade ensure that you have performed all the steps in [Before upgrading software](#) to ensure that the critical data is backed-up so that it can be restored after the upgrade.

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

4. If you are not re-installing the product, delete the configuration file **/etc/nfast.conf** if it exists.
5. Unless they are needed for a new installation, remove the user and group **nfast** and, if they exist, the user and group **ncsnmpd**.

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

6. If the file **nCipherKM.jar** is present, it is located in the extensions folder of your local Java Virtual Machine. The uninstall process may not delete this file and you may have to remove it manually.

6. System upgrade

Terms used in this topic

software

Security World software running on the PC in which the HSM is installed

firmware

Security World firmware running on the HSM

You can upgrade **software** and **firmware** independently of each other.

6.1. Software and firmware compatibility

In general, Entrust recommends that you use the software and firmware from the same version of Security World. The system is designed to be backwards compatible so that it will still operate with differing versions of software and firmware but some functionality may not be available and you may receive warnings during operation.

This user guide describes the behaviour of v13.5 software interacting with v13.5 firmware. Some areas where functionality differs depending on the version of firmware loaded are also described in this guide but it is not possible to describe all possible combinations of software and firmware.

Release notes and user guides for each Security World release are available from the Entrust website and these together with Entrust Support will help you should you experience any problems when operating with differing versions of software and firmware.

6.2. System upgrade procedure

When upgrading the whole system, Entrust recommends that you always upgrade the host software before upgrading the HSM firmware, however this is not mandatory and you may upgrade the firmware first should you wish to do so.



Always read the release notes accompanying the Security World release before upgrading any part of the system as these may include additional upgrade steps.



If the Version Security Number (VSN) of the firmware has been increased, it may not be possible to roll-back the firmware to the previous version after upgrade. See [Version Security Number](#) for more

information.

6.3. Upgrade software

For Security World software upgrades, you do not need to delete key data or any existing Security World. 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) available.

6.3.1. Before upgrading software

You must perform these steps if you are planning to re-install the Security World software, for example to re-install it on the same machine after an operating system update, or to install a newer Security World software version as part of an upgrade.

Performing these steps is useful even if you are not planning a re-install because it preserves data that you would otherwise irretrievably lose when you uninstall the Security World software.

1. **(Only if you are using the nShield PKCS #11 library)** Back up the `cknfastrc` file by copying it to external media or to a location not within the Security World installation.
2. **(Linux only)** Back up your Security World and nShield configuration files stored in `/opt/nfast/kmdata/` and `/opt/nfast/hardserver.d` by copying them to external media or to a location not within `/opt/nfast`.

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

3. **(nShield 5s only)** Back up your SSH keys, see [Making a backup of installed SSH keys](#):
 - If you are planning a clean reinstallation of the Security World software on the **same machine and same operating system**, back up your SSH keys in `/opt/nfast/services` using `hsmadmin keys backup`.
 - If you are planning to re-create the Security World on a **different machine or after re-installing the operating system**, use `hsmadmin keys backup --passphrase`. `hsmadmin keys backup` alone is only suitable for a local backup followed by a local restore on the same machine and same operating system.



If you erase your SSH keys without making a backup you will need

to use recovery mode, see [Recovery mode](#) to restore communication with the HSM. This will return the HSM to factory state, see [Factory state](#).

6.3.2. Reinstall Security World software

Software upgrade is performed by uninstalling the old software as described in [Uninstalling Security World Software](#) and then installing the new software as described in [Install the Security World software](#).

6.3.3. After upgrading software

1. Copy back any data that was manually backed-up as part of the procedures in [Before upgrading software](#) to the locations from which it was copied.
2. (**nShield 5s only**) Restore communication with the HSM by following the procedures at [restoring SSH keys from backup](#).

6.4. Upgrade firmware

See the following pages for instructions on upgrading the firmware:

- [Upgrading the image file and associated firmware: network-attached HSMs](#)
- [Upgrade firmware: nShield Solo, Solo XC, and Edge HSMs](#)
- [Upgrade firmware: nShield 5s](#)

7. Software packages on the installation media

This guide lists the contents of the component bundles and the additional software supplied on your Security World Software installation media.

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

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

7.1. Security World installation media

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

Linux Package	Windows Feature in the Installer	Content
<code>hwsp</code>	nShield Hardware Support	Hardware Support package, including the nShield Server and the most essential setup tools including enquiry, nfkminfo, and the Remote Administration Client command line tool. On Linux this also contains the PCIe HSM device drivers.
<code>ctls</code>	nShield Core Tools	Management utilities, including generatekey, diagnostic, OpenSSL, performance tools, the nShield Remote Administration GUI tool, and the PKCS#11 library.
<code>ctd</code>	nShield CipherTools	Developer package example programs, and developer libraries for the nCore, SecurityWorld and PKCS#11 APIs for C/C++ and Python.
<code>devref</code>	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 executables.
N/A	nShield Device Drivers	Device drivers for PCI and USB attached nShield devices, included in <code>hwsp</code> for Linux.

Linux Package	Windows Feature in the Installer	Content
<code>javasp</code>	nShield Java	nCipherKM JCA/JCE Provider, associated classes (including nFast Java generic stub classes) and the KeySafe application.
<code>jd</code>	nShield Java Developer	Java developer libraries and documentation for the nCore API and generic stub.
<code>ncsnmp</code>	nShield SNMP	nShield SNMP service and tools.
N/A	nShield Trusted Verification Device	Driver for the Trusted Verification Device (TVD), included in <code>ctls</code> for Linux.
<code>raserv</code>	nShield Remote Administration Server	nShield Remote Administration server for enabling communication between remote clients and their Type3 smartcards and this machine.