nShield Security World

nShield Edge v13.3 Install Guide

18 October 2024

Table of Contents

1. Introduction . . . 1
    1.1. About this guide . . . 1
    1.2. Terminology . . . 1
2. Safety and security . . . 2
    2.1. FIPS . . . 2
3. Regulatory notices . . . 3
    3.1. FCC class A notice . . . 3
    3.2. Canadian certification - CAN ICES-3 (A)/NMB-3(A) . . . 3
    3.3. Recycling and disposal information . . . 3
4. Before you install the software . . . 4
    4.1. Preparatory tasks before installing software . . . 4
        4.1.1. Windows . . . 4
        4.1.2. Linux . . . 4
        4.1.3. All environments . . . 5
    4.2. Firewall settings . . . 6
5. Installing the software . . . 8
    5.1. Installing the Security World Software on Windows . . . 8
    5.2. Installing the Security World Software on Linux . . . 9
6. Setting up the nShield Edge . . . 11
    6.1. Power saving options . . . 11
    6.2. Connecting an nShield Edge . . . 11
        6.2.1. Windows . . . 11
        6.2.2. Linux . . . 12
    6.3. Enabling optional features . . . 12
    6.4. Disconnecting and reconnecting the nShield Edge . . . 12
    6.5. Checking the installation . . . 13
    6.6. Using a Security World . . . 13
7. Using the nShield Edge . . . 14
    7.1. Mode LEDs . . . 14
    7.2. Changing the mode . . . 15
    7.3. Status LED . . . 15
8. Troubleshooting . . . 16
    8.1. None of the LEDs are lit . . . 16
    8.2. The Mode LED is amber or red . . . 16
    8.3. The Status LED is flashing irregularly and the nShield Edge is unresponsive for more than a few minutes . . . 16
    8.4. The Security World Software does not detect the connected nShield Edge . . . 16

8.5. Upgrading the firmware . . . 16
9. nShield Edge Windows compatibility issues and considerations . . . 17
9.1. nShield Edge very slow in VMware virtual machine . . . 17
10. Dimensions and operating conditions . . . 18
10.1. Physical location considerations . . . 18
11. Uninstalling existing software . . . 19
11.1. Uninstalling the Security World Software on Windows . . . 20
11.2. Uninstalling the Security World Software on Linux . . . 20
12. Software packages . . . 22
12.1. Security World installation media . . . 22
12.1.1. Component bundles . . . 22
12.2. Components required for particular functionality . . . 23
12.2.1. KeySafe . . . 23
12.2.2. Microsoft CAPI CSP and Microsoft Cryptography API: Next Generation (CNG) . . . 23
12.3. nCipherKM JCA/JCE cryptographic service provider . . . 24
12.4. SNMP monitoring agent . . . 24

1. Introduction

The Entrust 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 highvalue 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.

Entrust does not recommend using the nShield Edge alongside other Entrust nShield HSMs on the same computer or VM.

1.1. About this guide

This guide includes:

- Installing the Security World Software. See Installing the software.
- Steps to set up an nShield Edge. See Setting up the nShield Edge.
- How to use an nShield Edge. See Using the nShield Edge.
- Troubleshooting information. See Troubleshooting.
- nShield Edge compatibility considerations. See nShield Edge Windows compatibility issues and considerations.
- Instructions to uninstall existing software. See Uninstalling existing software.
- Software components and bundles. See Software packages.

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

1.2. Terminology

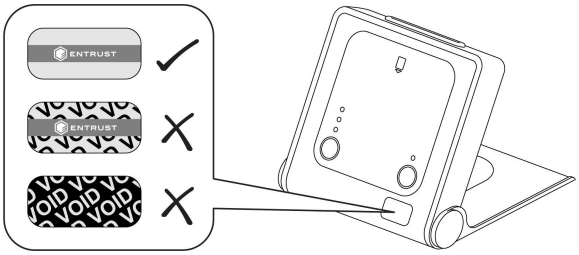
The nShield Edge is referred to as *the nShield Edge*, *the Hardware Security Module*, or *the HSM*.

2. Safety and security

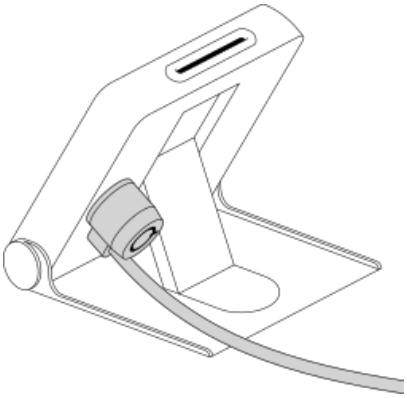
There are no user-serviceable parts inside the nShield Edge. Any attempt to dismantle the nShield Edge results in any remaining warranty cover, the maintenance and support agreement, or both being rendered void.

To help maintain security:

- Always inspect the USB cable and the nShield Edge before use, specifically the Entrust 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.



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



- Never store or carry smart cards with the nShield Edge.
- Protect your passphrase 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 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

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

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.
- If the nShield Remote Administration Client is installed on the machine, remove it. You will also have to re-install it after you installed the new Security World software version. See the *nShield Remote Administration User Guide*.

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

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. Linux

4.1.2.1. 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.

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.

  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.

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 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.

4.1.3.2. 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.

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, and 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.

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	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 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 *nShield Solo, Solo XC, and nShield Edge User Guide* 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 *nShield Solo, Solo XC, and nShield Edge 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 on Windows

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.
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. In the drop-down menu, deselect the components you do not want to install. **nShield Hardware Support** and **Core Tools** are necessary to install the Security World Software.

   See Software packages 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 the Windows Start menu: **Start > Entrust nShield Security World**:

   - 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 *nShield Solo, Solo XC, and nShield Edge User Guide*.

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

   The following global variables are set upon install:

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

5.2. 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. 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

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:

Windows

1. From the **Power Options** section of the Control Panel, select **Power Option > Change plan settings**.
2. For **Put the computer to sleep**, select **Never**.

Linux

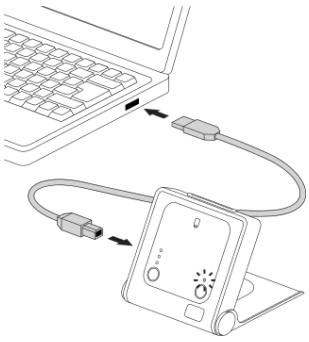
Set power options to never put computer to sleep.

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.



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

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

6.2.2. Linux

1. Connect the nShield Edge to your computer, using the supplied USB cable.
2. Open a terminal window and enter the following command:

```
>tail -f /opt/nfast/log/edgeHandler.log
```

A message appears in the log file, reporting that Linux is stopping and restarting the hardserver. This takes approximately 30 seconds.

For example:

```
2020-01-09 10:33:35 INFO: Waiting for the Edge to be ready: ETA 30 seconds
2020-01-09 10:34:05 WARN: Restarting hardserver
waiting for nCipher server to become operational ...
nCipher server now running
2020-01-09 10:34:09 INFO: The hardserver has finished restarting
```

When the hardserver has restarted, you are ready to use the nShield Edge with the Security World Software. See the *nShield Solo, Solo XC, and nShield Edge 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 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 Entrust.

To enable optional features, follow the instructions in the *nShield Solo, Solo XC, and nShield Edge 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
```

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.

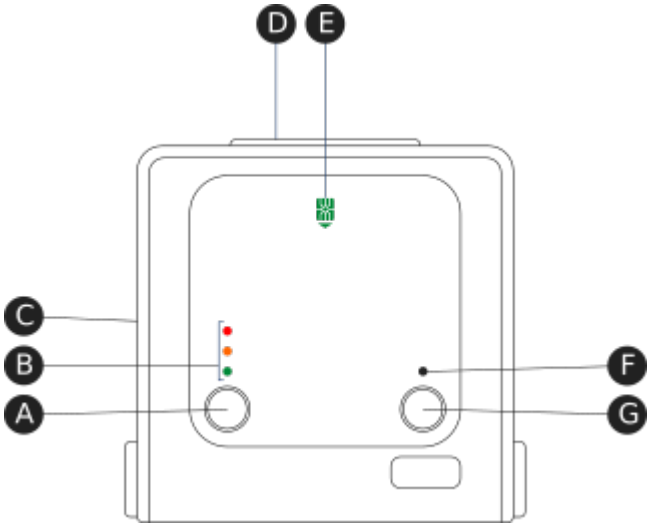
Ensure that the Windows power saving features are disabled. See Power saving options for more information.

6.6. Using a Security World

See the *nShield Solo, Solo XC, and nShield Edge User Guide* for more about creating a Security World or loading an existing one.

7. Using the nShield Edge

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 https://nshieldsupport.entrust.com.

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 hardserver by following the instructions in the *nShield Solo, Solo XC, and nShield Edge User Guide*.

8.5. Upgrading the firmware

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

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). This can 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_dtpp_devices=COM2`, specifying the COM port number of the new serial port in the VM. Make sure this is the only line with `serial_dtpp_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

Entrust nShield HSMs are certified to NIST FIPS 140 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.

11. Uninstalling existing software

Entrust 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, Entrust strongly recommends that you make a secure backup of any existing Security World and nShield configuration files. See the *nShield Solo, Solo XC, and nShield Edge 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 *nShield Solo, Solo XC, and nShield Edge 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 *nShield Solo, Solo XC, and nShield Edge User Guide* 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.

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 *nShield Connect User Guide* section *Configuring the nShield Connect to use the client* for more information.

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

> intend to upgrade it.

11.1. Uninstalling the Security World Software on Windows

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

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

11.2. Uninstalling the Security World Software on Linux

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

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

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

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

   ```
   $ su -
   ```

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

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

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

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

5. If you are not 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.

1. Unless needed for a subsequent installation, remove the user `nfast` and, if it exists, the user `ncsnmpd`:
   a. `userdel -r nfast` and `userdel -r ncsnmpd` will remove the users.
   b. `groupdel nfast` and `groupdel ncsnmpd` will remove their groups.

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

12. Software packages

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.

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

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

12.1. Security World installation media

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

12.1.1. Component bundles

Linux Package	Windows Feature in the Installer	Content
`hwsp`	nShield Hardware Support	Hardware Support package, including the nShield Server and device driver.
`ctls`	nShield Core Tools	Management utilities, including generatekey, diagnostic and performance tools, Remote Administration Client tools, and the PKCS#11 library.
`ctd`	nShield CipherTools	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 executables.
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.

12.2. Components required for particular functionality

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

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

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

In these part codes, n represents any integer.

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

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

12.2.1. KeySafe

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

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

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

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

- The *nShield Solo, Solo XC, and nShield Edge User Guide*.
- The appropriate third-party integration guide for your application.

Entrust has produced *Integration Guides* for many supported applications. The *Integration Guides* describe how to install and configure an application so that it works with Entrust hardware security modules and Security Worlds. For more information about the Entrust range of *Integration Guides*:

- Visit https://www.entrust.com/documentation.
- Contact Support: https://nshieldsupport.entrust.com.

12.3. nCipherKM JCA/JCE cryptographic service provider

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

- The nShield Java bundle

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

See the *nShield Solo, Solo XC, and nShield Edge User Guide* for more about configuring the nCipherKM JCA/JCE cryptographic service provider.

12.4. SNMP monitoring agent

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

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

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

See the *nShield Solo, Solo XC, and nShield Edge User Guide* for more about how to activate the SNMP agent after installation.