nShield Security World

nShield Solo v12.81 Install Guide

12 July 2024

Table of Contents

1. Introduction

The Entrust nShield Solo, Solo XC, and nShield 5s are Hardware Security Modules (HSM) for servers and appliances.

1.1. About this guide

This guide includes:

- Installing the nShield Solo, nShield Solo XC, and nShield 5s. See Installing the module.
- Installing the Security World Software. See Installing the software.
- Steps to check the installation. See Checking the installation.
- 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
- The advanced features of an nShield Solo, nShield Solo XC, and nShield 5s.

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
xC3*xxx*E-*xxx* xC4*xxx*E-xxx	nShield Solo PCIe
xC30*x*5E-*xxx* xC40*x*5E-*xxx*	nShield Solo XC PCIe
NC5536E-*n*	nShield 5s PCIe F3

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 and enabling additional features (such as client licenses), see the *nShield Solo, nShield Solo XC and nShield Edge - User Guide*. Entrust strongly recommends that you read the release notes at https://nshieldsupport.entrust.com. These notes contain the latest information about your product.

1.4. Terminology

The nShield Solo, nShield Solo XC, and nShield 5s are referred to as a the *nShield Solo*, *nShield Solo XC*, and *nShield 5s*, the *Hardware Security Module*, or the *HSM* in this guide.

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. Battery cautions

Danger of Explosion if the battery is incorrectly replaced. The battery may only be replaced with the same or equivalent type. Dispose of the used battery in accordance with your local disposal instructions.

3.4. Hazardous substance caution

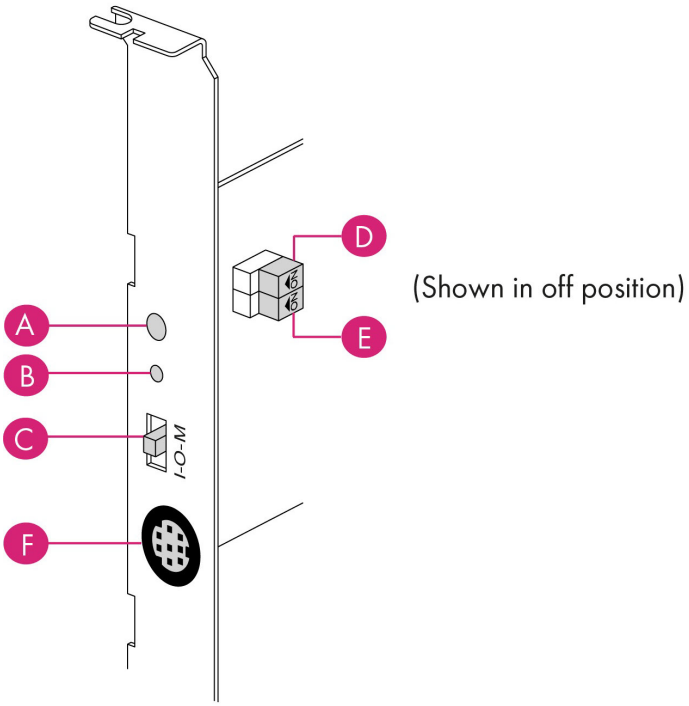
This product contains a lithium battery and other electronic components and materials which may contain hazardous substances. However, this product is not hazardous providing it is used in the manner in which it is intended to be used.

3.5. Recycling and disposal information

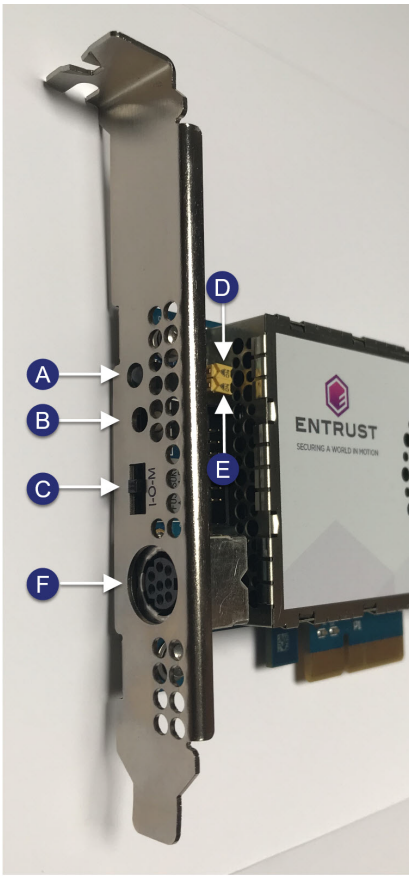
For recycling and disposal guidance, see the nShield product's *Warnings and Cautions* documentation.

4. Before installing the module

4.1. Back panel and jumper switches



nShield Solo



nShield Solo XC

Label	Description
A	Status LED
B	**Solo, Solo XC**: Recessed clear button **nShield 5s**: Recovery mode button
C	Physical mode switch
D	Physical mode override jumper switch, in the **Off** position. When set to **On**, the mode switch (C) is deactivated. See the *User Guide* for more information.
E	Remote mode override jumper switch, in the **Off** position. When set to **On**, remote mode switching is disabled. See the *User Guide* for more information.
F	A mini-DIN connector for connecting a smart card reader.

The configuration of connectors varies between modules and might not

> be as in the image.

4.2. 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.
- If you intend to install the module with an external smart card reader, check the cable for signs of tampering. If evidence of tampering is present, do not use and request a new cable.
- **Solo and Solo XC only**

  Check that the two jumper switches are in the required positions.

- The physical mode switch must be set to Operational (**O**) to be able to use the remote mode switch override to change the mode. To use the Remote Administration feature to be able to change the mode of the module remotely, ensure that the jumper switch (**E**) is in the off position and the physical mode switch (**C**) is set to Operational (**O**).

The default factory setting of the jumper DIP switch **E** is **Off**. This enables remote MOI switching. Factory shipping nShield Solo HSMs loaded with firmware 2.61.2 or greater will support remote MOI switching by default. Customers who expressly do not want to enable the remote MOI switching capability must switch jump switch **E** to the **On** position.

4.3. 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.

4.4. Replace the fan - Solo XC only

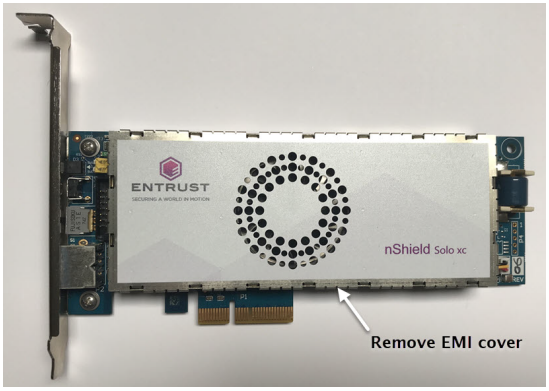
Required Tools

- Phillips screwdriver #0
- Phillips screwdriver #2
- Small needle nose pliers

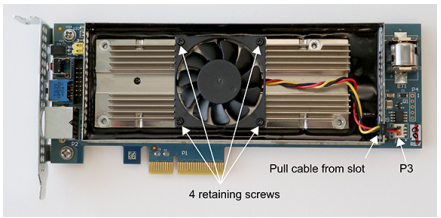
Required Part

- Orderable part number SOLOXC-REP-FAN (Replacement fan assembly).

1. Power off the system and while taking ESD precautions, remove the Solo XC card.
2. Place the Solo XC on a flat surface.
3. Remove the top EMI cover using a #2 screwdriver.

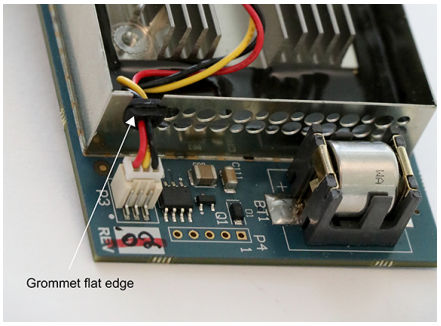


4. Pull the fan power cable and grommet from the slot in the EMI fence.
5. Using the needle nose pliers, gently remove the fan power cable from the P3 connector.



6. Using the #0 Phillips screwdriver, remove the four fan retaining screws.
7. Remove the defective fan from the Solo XC and install the replacement fan with the power cable positioned towards the P3 power connector. Ensure that the fan lays flat against the heatsink.
8. Replace the four fan retaining screws.
9. Install the power cable connector into the Solo XC P3 power connector.
10. Install the power cable grommet into the slot in the EMI fence, with the flat side

towards the top of the fence.



11. Replace the top EMI cover.
12. Re-install the Solo XC into the PCIe slot.

4.5. Replace the battery - Solo XC and nShield 5s

Please follow battery disposal guidelines in the installation manual.

Required tools

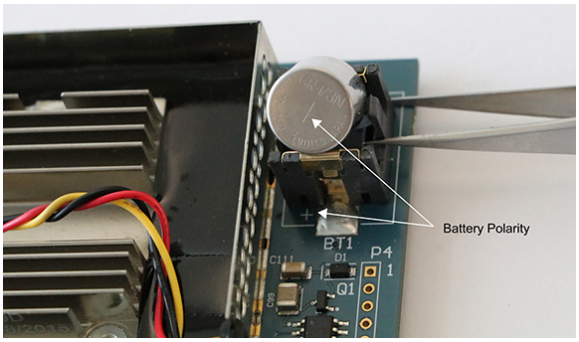
- Small non-conductive tweezers

Required part for both Solo XC and nShield 5s

- Orderable part number: SOLOXC-REP-BATT (Replacement battery)

To remove and replace the battery:

1. Power off the system and while taking ESD precautions, remove the module.
2. Place the module on a flat surface.
3. Using the tweezers, gently remove the battery from the BT1 connector.



4. Observing the polarity, install the replacement battery in the BT1 connector.
5. Re-install the module into the PCIe slot.

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 nShield Solo or nShield Solo XC module into a PCI slot. See the instructions that your computer manufacturer supplied to correctly identify the slots on your computer.

   Minimum requirement:

nShield Solo	1 PCIe x1 slot
nShield Solo XC	1 PCIe x4 slot
nShield 5s	1 PCIe x4 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. **Solo and Solo XC only**

   Check that the two jumper switches on the module are still in required positions (see Back panel and jumper switches).

7. **Solo and Solo XC only**

   Check that the mode switch is still in the center **O** (operational) position.

8. Replace the computer case.

5.1. Fitting a smart card reader

Connect the smart card reader to the connector on the back panel of the module. A D-type to mini-DIN adapter cable is supplied with the module.

5.2. 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

Before you install the software, you should:

- Install the module. See Installing the module.
- Uninstall any older versions of Security World Software. See Uninstalling existing software.
- Complete any other necessary preparatory tasks, as described in Preparatory tasks before installing 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.

You may also need to set power management properties of the nShield Solo, once the Security World Software is installed. See Installing the Security World Software on Windows for more information.

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.

You need to install the Remote Administration Service component if you require remote administration functionality. See Preparatory tasks before installing software and the *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 Security World installation media for more about optional components.

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
Hardserver	9004	Incoming impath connections from other hardservers, for example: • From a cooperating client to the remote file system it is configured to access • From a non-attended host machine to an attended host machine when using Remote Operator
Remote Administration Service	9005	Incoming connections from Remote Administration Clients
Audit Logging syslog	514	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

If you are using an nShield Edge as a Remote Operator slot for an HSM located elsewhere, you need to open port 9004. You may restrict the IP addresses to those you expect to use this port. You can also restrict the IP addresses accepted by the hardserver in the configuration file. See the *User Guide* for your module and operating system for more about configuration files. Similarly, if you are setting up the Remote Administration Service you need to open port 9005.

7. Installing the software

This chapter describes how to install the Security World Software on the host computer.

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.

   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. 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*.

Do not run any CSP installation wizard before installing the module hardware.

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

In the following instructions, *disc-name* is the name of the mount point of the installation media.

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.

   See Software packages on the Security World installation media for more about the component bundles and the additional software supplied on your installation media.

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. Checking the installation

This section describes what to do if you have an issue with the module or the software.

The facilities described below are only available if the software has been installed successfully.

8.1. Checking operational status

8.1.1. Enquiry utility

Run the `enquiry` utility to check that the module is working correctly. You can find the `enquiry` utility in the `bin` subdirectory of the `nCipher` directory. This is usually:

- `C:\Program Files\nCipher\nfast` for Windows
- `/opt/nfast` for Linux

If the module is working correctly, the `enquiry` utility returns a message similar to the follow ing:

nShield Solo

```
Server:
enquiry reply flags    none
enquiry reply level    Six
serial number          #############-####
mode                   operational
version                #.#.#
speed index            ###
rec. queue             ##..##
...
version serial         #
remote server port     ####
...
module type code       0
product name           nFast server
...
Module ##:
enquiry reply flags    none
enquiry reply level    Six
serial number          #############-####
mode                   operational
version                #.#.#
speed index            ###
rec. queue             ##..##
...
module type code       7
product name           #######/#######/#######
...
rec. LongJobs queue    ##
SEE machine type       Power PCSXF
supported KML types    DSAp1024s160 DSAp3072s256
```

```
hardware status        OK
```

nShield Solo XC

```
Server:
enquiry reply flags    none
enquiry reply level    Six
serial number          #############-####
mode                   operational
version                #.#.#
speed index            ###
rec. queue             ##..##
...
module type code       0
product name           nFast server
...
version serial         #
remote server port     ####

Module ##:
enquiry reply flags    none
enquiry reply level    Six
serial number          #############-####
mode                   operational
version                #.#.#
speed index            ###
rec. queue             ##..##
...
module type code       12
product name           ########/########/########
...
rec. LongJobs queue    ##
SEE machine type       Power PCELF
supported KML types    DSAp1024s160 DSAp3072s256
hardware status        OK
```

nShield 5s

```
Server:
enquiry reply flags  none
enquiry reply level  Six
serial number        #############-####
mode                 operational
version              #.#.#
speed index          ###
rec. queue           ##..##
...
module type code     0
product name         nFast server
...
Module ##:
enquiry reply flags  none
enquiry reply level  Six
serial number        #############-####
mode                 operational
version              #.#.#
speed index          ###
rec. queue           ##..##
...
module type code     14
product name         ########/########
...
```

```
rec. LongJobs queue  ##
SEE machine type     None
supported KML types  DSAp1024s160 DSAp3072s256
active modes         none
hardware status      OK
```

If the mode is operational the module has been installed correctly.

If the mode is initialization or maintenance, the module has been installed correctly, but you must change the mode to operational. See the *User Guide* for your module and operating system for more about changing the module mode.

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 and higher versions, ensure that the power saving features are disabled. See Installing the module for more information. Otherwise, if your system enters Sleep mode, the nShield Solo module may not be found when running `enquiry`. If this hap pens, you need to reboot your system.

8.1.2. nFast server (hardserver)

Communication can only be established with a module if the nFast server is running. If the server is not running, the `enquiry` utility returns the message:

```
NFast_App_Connect failed: ServerNotRunning
```

Restart the nFast server, and run the `enquiry` utility again. See the *User Guide* for more about how to restart the nFast server.

8.2. Mode switch and jumper switches

The mode switch on the back panel controls the mode of the module. See the *User Guide* for more about checking and changing the mode of an HSM. You can set the physical mode override jumper switch on the circuit board of the nShield Solo to the **On** position, to pre-vent accidental operation of the mode switch. If this override jumper switch is on, the nShield Solo and nShield XC Solo XC will ignore the position of the mode switch (see Back panel and jumper switches).

You can set the remote mode override jumper switch on the circuit board of the nShield Solo and nShield Solo XC to the **On** position to pre vent mode change using the `nopclearfail` command. This should be

> done if, for example, the security policies of your organization require the physical mode switch to be used to authorize mode changes.

8.3. Log message types

By default, the hardserver writes log messages to:

- The event log in Windows Operating Systems.
- `log/logfile` in the `nCipher` directory (normally `opt/nfast/log` directory) on Linux. The environment variable `NFAST_SERVERLOGLEVEL` determines what types of message you see in your log. The default is to display all types of message. For more information on `NFAST_SERVERLOGLEVEL`, see the *User Guide*.

> `NFAST_SERVERLOGLEVEL` is a legacy debug variable.

8.3.1. Information

This type of message indicates routine events:

```
nFast Server service: about to start
nFast Server service version starting
nFast server: Information: New client clientid connected
nFast server: Information: New client clientid connected - privileged
nFast server: Information: Client clientid disconnected
nFast Server service stopping
```

8.3.2. Notice

This type of message is sent for information only:

```
nFast server: Notice: message
```

8.3.3. Client

This type of message indicates that the server has detected an error in the data sent by the client (but other clients are unaffected):

```
nFast server: Detected error in client behaviour: message
```

8.3.4. Serious error

This type of message indicates a serious error, such as a communications or memory failure:

```
nFast server: Serious error, trying to continue: message
```

If you receive a serious error, even if you are able to recover, contact Support.

8.3.5. Serious internal error

This type of message indicates that the server has detected a serious error in the reply from the module. These messages indicate a failure of either the module or the server:

```
nFast server: Serious internal error, trying to continue: message
```

If you receive a serious internal error, contact Support.

8.3.6. Start-up errors

This type of message indicates that the server was unable to start:

```
nFast server: Fatal error during startup: message nFast Server service version failed init.
nFast Server service version failed to read registry
```

Reinstall the server as described in the *User Guide* for your module type. If this does not solve the problem, contact Support.

8.3.7. Fatal errors

This type of message indicates a fatal error for which no further reporting is available:

```
nFast server: Fatal internal error
```

or

```
nFast server: Fatal runtime error
```

If you receive either of these errors, contact Support.

8.4. Utility error messages

8.4.1. BadTokenData error

The PCIe module (not the Solo XC module) is equipped with a rechargeable backup battery for maintaining Real-Time Clock (RTC) operation when the module is powered down. This battery typically lasts for two weeks. If the module is without power for an extended period, the RTC time is lost. When this happens, attempts to read the clock (for example, using the `ncdate` or `rtc` utilities) return a `BadTokenData` error status.

The correct procedure in these cases is to reset the clock and leave the module powered up for at least ten hours to allow the battery to recharge. No other nonvolatile data is lost when this occurs. See the *Solo User Guide* for more about resetting the clock.

The Solo XC module is equipped with a battery with a ten year life for maintaining RTC oper ation when the module is powered down. The RTC will not require resetting after the mod- ule has been shut down for extended periods. The battery is not rechargeable.

Solo XC only: Reboot the Solo XC for the firmware upgrade to take effect.

Linux bare metal environments: With the module in Maintenance mode, run the following command to reboot the Solo XC:

```
nopclearfail -S -m<module_number>
```

Linux virtual environment hosts and Windows:

Reboot the system that is hosting the Solo XC.

On all platforms:

Wait for the Solo XC to reboot. The module has completed rebooting when running `enquiry` no longer shows the module as Offline.

9. Status indicators

9.1. 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.
Flashes two short pulses, followed by a short pause.	`Status: Initialization mode` Used to create and load Security World data on the HSM and to erase Security World from the HSM and return it to factory state.
Flashes two long pulses followed by a pause.	`Status: Maintenance mode` Used for reprogramming the module with new firmware. The module only goes into Maintenance mode during a software upgrade.
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. For nShield Solos and nShield Solo XCs running firmware Remote Administration 2.61.2 and above, the error code is also reported by the `enquiry` utility in the `hardware status field` of the `Module`. 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*.

Use the mode switch to move between Maintenance, Operational, and Initialization modes. See Mode switch and jumper switches for more information.

10. Uninstalling existing software

Entrust recommends that you uninstall any existing older versions of Security World Software before you install new software. In Windows environments, 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. However, on Linux, a manual installation using `.tar` files *does* overwrite existing data and directories.

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.
`redist`	N/A	Contains the redistributable GNU C and C++ shared libraries.

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

12. Virtualization Remote Server

The nShield Solo XC is compatible with the leading server virtualization and hypervisor man agement platforms, including:

Virtualization provides an environment where multiple operating systems can run at the same time on one physical computer. Each virtual machine is an isolated, virtualized com- puter system that can run its own operating system.

- **Microsoft Hyper-V**, a role in Windows Server used to create and manage a virtualized server computing environment
- **VMware vSphere / ESXi**, a robust, bare-metal hypervisor that installs directly onto your physical server.

  All vSphere management functions are performed through remote management tools.

- **Citrix XenServer** - includes the XenCenter management console.

  PCI passthrough is configured using the XenCenter software with command line tools and utilities. PCI passthrough allows a VM client direct access to the nShield Solo XC.

The operating system that runs within a virtual machine is referred to as a *guest operating system*.

nShield software includes the nShield hardserver applications. These applications enable applications running on multiple virtual guest operating systems to all share nShield Solo XC hardware.

Hardserver processing services can be shared among multiple virtual operating system instances as long as each instance has hardserver installed. Inside of the operating system, hardservers can communicate with other hardservers.

12.1. Virtualization and Hyper-V

The host hardserver is configured to run on the Parent/Dom0 operating system. The Par- ent/Dom0 operating system has privileged access to the Solo XC hardware over the PCI bus.

Instead of using a physical network for communication between the VM guest instances running on the same physical system, most hypervisors provide the capability to instantiate some form of virtual switch which allows the network communication to take place between the VMs entirely within the hypervisor software. This means that nCore data does not need to be routed outside of the server hardware.

12.2. Virtualization and XenServer/VMware vSphere hypervisor, ESXi

ESXi and XenServer do not use the concept of a Parent/Dom0 VM. Instead, an additional VM is defined in the system as the host with passthrough permissions to enable access to the nShield Solo XC.

12.3. ESXi environment

After installing VMware ESXI, the VM guest can be remotely managed and the PCI passthrough of the Solo module configured using vSphere. PCI passthrough allows a VM guest direct access to the nShield Solo XC.

12.3.1. Set up a basic single-node vCenter server instance

Follow the steps below to use the vCenter Simple Install to set up a basic single-node vCenter Server instance. You will install the vSphere Web Client and use its in-browser interface to add ESXi hosts to your vSphere inventory.

1. Log on the system as administrator and start at least one ESXi host.
2. Install ESXi using the vCenter Simple Install option using the instructions provided in the VMware vSphere documentation (https://docs.vmware.com/en/VMware-vSphere/index.html).
3. Install the vSphere Web Client using the instructions provided in the VMware vSphere documentation.

12.3.2. Configure passthrough devices on a host

Follow the steps below to add ESXi hosts to the vCenter Server inventory, in order to create a vSphere environment and use vSphere features.

1. Enter the IP address, username and root password of your host created when you installed ESXi.
2. Select **Login**, the **Getting Started** page will be displayed.
3. Select the **Configuration** tab.
4. Select **Advanced Settings**.
5. Select **Configure Passthrough**. The **Passthrough Configuration** page is displayed listing all available passthrough devices.

6. Select **Edit**.
7. Select the check box to mark the endpoint for passthrough.

   For example, the check mark box for 02:00.0 will be **Freescale Semiconductor Inc <class> Power PC**.

8. Select **OK**.

ESXi will now be successfully installed and the Solo PCIe module has been configured for passthrough.

12.3.3. Create the VM guest instance

VMware ESXi provides the capability of PCI passthrough and it is a bare metal Hypervisor. This requires the creation of two or more guests which communicate via Vswitch. One of the guest will act as the primary guest and will be configured as described below utilizing the PCI card connected via passthrough. The second and subsequent guests can be composed of the identical configuration with the exception of the PCI passthrough connection.

To create the VM guest instance:

1. Navigate to **File > New > Virtual Machine** in the vSphere Client. A wizard will prompt you through each of the settings displayed in the working pane.
2. Select **Typical Configuration** and then select **Next**.
3. Enter a name and select **Next**.
4. Select a storage device for the VM files.
5. Select a Guest Operating System (OS) and an OS version from the drop down menu.
6. Select **Next**.
7. Configure the network connections as follows:
   a. How many NICs do you want to connect? **1**.
   b. Network: **VM Network**.
   c. Adapter: **VMXNET 3**.
   d. Connect at Power On: ✓.
8. Select **Next**.
9. Configure the virtual disk size for the guest VM as follows:

It is important to select the same network configuration for both the guest primary VM and the guest secondary VM, as it is a require ment for IP communication between the two.

a. Datastore: **<datastore1>**.
b. Available space (GB): **<357.3>**.
c. Virtual disk size: **50 GB**.
d. Select **Thick Provisioned Lazy Zeroed**.

10. Select **Next**.
11. Select **Edit the virtual machine settings before completion**.
12. Select **Continue**.
13. Select **Add**.
14. Select **PCID**.
15. Select **Next**.
16. Select the configured PCI passthrough device.

    For example, 02:00.0 will be **Freescale Semiconductor Inc <class> Power PC**.

17. Select **Next**.
18. Select **Finish**.

12.4. XenServer environments

Install the XenServer, follow the instructions in the *Citrix XenServer Quick Start Guide*, see https://docs.citrix.com/en-us/xenserver.

12.4.1. Configure the XenCenter client

To remotely manage VM guests and configure PCI passthrough of the nShield Solo XC:

1. Enter the XenServer web client IP address.
2. Select **XenCenter installer**. The XenCenter software will auto install.
3. Select the XenServer that you want to connect to and manage from the Resources pane. A connection is established providing access to all the VMs installed on the server.
4. Select the **Console** tab from the **Properties** tabs pane.

Dom0 is the initial domain started by the Xen hypervisor on boot. Dom0 runs the Xen management toolstack and is has direct access to the hardware. Dom0 provides Xen virtual disks and network access for VM guests, each VM guest is referred to as a DomU (that is, an unprivileged domain).

5. Run the command `lspci`.

   A detailed list of all the PCI buses and devices in the system is displayed, for example:

   ```
   02:00.0 Power PC:  Freescale Semiconductor Inc Device 082c (rev11)02:00:0
   ```

   represents the nShield Solo XC card endpoint.

6. Open the file `/boot/extlinux.conf` and scroll to the dom0 linux kernel append section. Add the PCI slot as shown below with the following command:

   ```
   pciback.hide=(02:00.0)
   ```

   Newer versions of Citrix XenServer utilize:

   ```
   xen-pciback.hide=(xx:xx:x)
   ```

7. Scroll to the end of the file.
8. Run the command:

   ```
   pciback.hide=<NG solo card endpoint>
   ```

   This command enters the PCI slot, for example:

   ```
   pciback.hide=(02:00.0) --- /boot/initrd-fallback.img
   ```

9. Save and close the file.
10. Run the command:

    ```
    extlinux -I /boot
    ```

11. Run the command:

    ```
    reboot
    ```

12. Run the command:

    ```
    xe vm-list
    ```

13. Locate the **uuid** using the VI Editor for the VM that you want to assign the PCI passthrough to.

14. Run the command:

```
xe vm-param-set other-config:pci=0/0000:<endpoint of the NG solo card> uuid: <uuid>
```

    This command adds the PCI device to the selected VM, for example:

```
xe vm-param-set other-config:pci=0/0000:02:00.0 uuid: 4a4ab965-a91d-70e7-2ec-a4c0004e1e8d
```

    If a PCI passthrough needs to be removed from a specific guest VM, run the command:

```
xe vm-param-clear param-name=other-config uuid=<vm uuid>
```

When the installation of XenCenter has completed, you can access [https://(XENSERVER-IP)] to acquire the corresponding XenCenter Client Remote management interface.

12.4.2. Create a XenServer guest instance and hardserver configuration

The XenServer is a bare metal Hypervisor that provides the PCI passthrough capability. As part of this process, you must create two **Dom U** guests that communicate through the Vswitch. One guest acts as the primary guest and is configured as described below utilizing the PCI card connected via passthrough. The second guest can be composed of the identical configuration with the exception of the PCI passthrough connection.

To create the first DomU guest VM:

1. Select the server from the **Resources** pane, right-click and select **New VM** from the dropdown menu.
2. Select a **Template**.
3. Select an **Operating system** for the first DomU guest VM.
4. Select **Next**.
5. Select **Name**.
6. Enter a name and select **Next**.

The DomU guest VM name will also be displayed in the XenCenter's Resources pane. You can change the name at any time.

7. Select **Installation Media**.
8. Select **Install from ISO library or DVD drive** and then select the appropriate media from the drop down menu.
9. Select **Next**.

10. Select **Home Server**.
11. Select **Place the VM on this server** and then select a home server from the drop down list of available servers.
12. Select **Next**.
13. Select **CPU & Memory** and enter the number of CPUs, chose your topology and enter an amount for memory.
14. Select **Next**.
15. Select **Storage**.
16. Select **Use these virtual disks:** and select a virtual disk from the display.
17. Select **Next**.
18. Select **Networking** and select the virtual network interface.
19. Select **Finish**.

If the guest VM is configured to have a PCI module via passthrough and the module is not connected to the VM instance, the guest VM instance will fail to power on. Verify that the Solo XC card is located on the same slot that was selected for the passthrough to the guest VM.

12.5. Hyper-V environment

The instructions assume there is a single nShield Solo XC module in the system.

The commands starting with `PS C:\>` should be run in PowerShell in elevated mode.

12.5.1. Set up

12.5.1.1. Install Hyper-V on the server

Follow the instructions in the Windows documentation for Hyper-V, see https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/.

12.5.1.2. Add the Hyper-V role to the server

To add the Hyper-V role in Windows server:

1. Log in as Administrator.

2. Open **Server Manager**.
3. Select **Manage**.
4. Select **Add Roles and Features**.
5. Select **Next**.
6. Select **Role-based or feature-based installation**.
7. Select **Next**.
8. Select **Select a server from the server pool**.
9. Select a server that has Windows 2016 installed. You will be adding Hyper-V to this server.
10. Select **Next**.
11. Select **Hyper-V**.
12. Select **Next**.
13. Reboot the system.

Once rebooted, Hyper-V will be supported by the Server 2016 instance.

12.5.1.3. Prepare the server

1. Enable the Input Output Memory Management Unit (IOMMU) policy on the server. This policy controls whether the Hyper-V server uses an IOMMU. To enable it, run the command:

```
bcdedit /set hypervisoriommupolicy enable
```

2. Check no devices are already set up for VM. Run the command:

```
PS C:\> Get-VMHostAssignableDevice
```

12.5.1.4. Prepare the device

1. Display the device address. Run the command:

```
PS C:\> (Get-PnpDevice -PresentOnly).Where{ $_.InstanceId -like '*VEN_1957*' } | Format-Table -autosize
```

2. Disable the device. Run the command:

```
PS C:\> Disable-PnpDevice -Verbose -InstanceId $instanceId -Confrm:$false
```

To find the `$instanceId` run the command:

```
PS C:\> $instanceId = (Get-PnpDevice -PresentOnly).Where{ $_.InstanceId -like
'*VEN_1957*' } | select -expand InstanceId
```

3. Dismount the device. Run the command:

```
PS C:\> $locationPath = Dismount-VmHostAssignableDevice -LocationPath $locationPath -Force -Verbose
```

To find the `$locationPath` run the command:

```
PS C:\> $locationPath = (Get-PnpDeviceProperty -KeyName
DEVPKEY_Device_LocationPaths -InstanceId $instanceId).Data[0]
```

4. Verify that the device is disabled and dismounted. Run the command:

```
PS C:\> Get-VMHostAssignableDevice
```

12.5.1.5. Install the Security World software

Install the Security World software suite into the operating system of the guest VM. Once the suite is installed, you can initialize the hardserver and then configure the guest VMs.

1. Insert the DVD-ROM containing the Security World software. The Security World software will auto install.
2. Run the `enquiry` utility to check that the module is working correctly. See Checking the installation.

12.5.1.6. Create the VM guest instance on the server

1. Open the Hyper-V Manager within your Windows 2016 server.
2. Log in as Administrator.
3. Navigate to **Action > New > Virtual Machine**.
4. Select **Next** (to create a virtual machine with a custom configuration).
5. Enter a name for the new guest VM instance.

Use the default location setting.

6. Select **Next**.
7. Select the OS generation to be installed on the new guest VM instance.

For example, **Generation 2** is selected. **Generation 2** is valid for products such as Windows 8 and beyond and with Windows Server

> 2016.

8. Select **Next**.
9. Select an amount of memory for allocation to this guest VM instance.
10. Select **Next**.
11. Select **Next**.
12. Select **Create a virtual hard disk**.
13. Enter **Name**, **Location** and **Size**.
14. Select **Next**.
15. Select one of the following options:
    - **Install an operating system later**, if you have a disk.
    - **Install an operating system from a bootable image file**, if you have the ISO path.
16. Select **Next**.
17. Select **Finish**.

12.5.1.7. Configure the VM guest instance on the server

1. Stop and select the VM guest instance. Run the commands:

```
PS C:\> $vmName = 'ws2016'

PS C:\> Stop-VM -VMName $vmName
```

2. Turn off the Automatic Stop Action. Run the command:

```
PS C:\> Set-VM -VMName $vm Name -AutomaticStopAction TurnOff
```

3. Make sure the memory minimum bytes match the memory startup bytes. Run the command:

```
PS C:\> Set-VM -VM $vm -DynamicMemory -MemoryMinimumBytes 4096MB -MemoryMaximumBytes 16384MB
-MemoryStartupBytes 4096MB
```

4. Assign a device to the VM guest instance. Run the commands:

```
PS C:\> Add-VMAssignableDevice -VM $vmName -LocationPath $locationPath -Verbose

PS C:\> Start-VM -VMName $vmName
```

> To find the $locationPath run the command:

```
PS C:\> $locationPath = (Get-PnpDeviceProperty -KeyName
DEVPKEY_Device_LocationPaths -InstanceId $instanceId).Data[0]
```

It is possible to assign the same device to a single VM guest instance multiple times. In this case the VM will not start. To check currently assigned devices, run the command below. To remove an assigned device see Remove a device from the VM guest instance.

```
PS C:\> Get-VMAssignableDevice -VMName $vmName
```

12.5.2. Remove a device from the VM guest instance

1. Remove a device from the VM. Run the commands:

```
PS C:\> $vmName = "ws2016"

PS C:\> Remove-VMAssignableDevice -Verbose -VMName $vmName}
```

12.5.3. Undo passthrough

1. Mount a single device. Run the command:

```
Mount-VMHostAssignableDevice -Verbose -LocationPath $locationPath
```

To find the `$locationPath` run the command:

```
PS C:\> $locationPath = (Get-PnpDeviceProperty -KeyName
DEVPKEY_Device_LocationPaths -InstanceId $instanceId).Data[0]
```

2. Enable a single device in device manager. Run the command:

```
Enable-PnpDevice -Confirm:$false -Verbose -InstanceId $instanceId
```

To find the `$locationPath` run the command:

```
PS C:\> $locationPath = (Get-PnpDeviceProperty -KeyName
DEVPKEY_Device_LocationPaths -InstanceId $instanceId).Data[0]
```