nShield Security World

nShield v13.6.16 Hardware Install and Setup Guides

26 May 2026

Table of Contents

1. Hardware install and setup guides

The hardware install and setup guides explain how to physically install and get started with your nShield HSMs.

The network-attached HSM install guide covers the following products:

- nShield 5c
- nShield Connect
- nShield 5c 10G

The PCIe install guide covers the following products:

- nShield 5s
- nShield Solo
- nShield Solo XC

The USB HSM setup guide covers the following products:

- nShield Edge

For instructions on installing the nShield Security World software, see nShield Security World Software v13.6.16 Installation Guide.

2. nShield Network-Attached HSMs

2.1. Prerequisites and product information

This guide covers the following HSMs:

- nShield Connect
- nShield 5c
- nShield 5c 10G

These Hardware Security Modules (HSMs) provide secure cryptographic processing within a tamper-resistant casing. Each nShield HSM is configured to communicate with one or more client computers over an Ethernet network. A client is a computer using the nShield HSM for cryptography. You can also configure clients to use other nShield HSMs on the net work, as well as locally installed HSMs.

- For further information about the HSM and HSMs in general, see nShield v13.6.16 HSM User Guide.
- For help installing the Security World software, see nShield Security World Software v13.6.16 Installation Guide.
- For guidance on using your HSM and the Security World software, see nShield Security World v13.6.16 Management Guide.
- For further information about compatible operating systems and virtual environments, see Compatibility in the release notes for the version of Security World you are using.

See Model numbers for a list of network-attached HSMs and their model numbers.

2.1.1. Power and safety requirements

The module draws up to 220 watts:

- Voltage: 100 VAC -240 VAC
- Current: 2.0 A - 1.0 A
- Frequency: 50 Hz - 60 Hz.

The module PSUs are compatible with international mains voltage supplies.

2.1.2. Weights and dimensions

Weight

11.5kg

Dimensions

43.4mm x 430mm x 690mm

The module is compatible with 1U 19” rack systems.

Measurements given are height x width x length/depth. If the inner slide rails are attached, the width of the unpackaged module is 448mm.

2.1.3. Handling the HSM

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

If you are installing the module in a 19" rack, make sure that you follow the instructions provided with the rails. In particular, be careful of sharp edges.

Only experienced personnel should handle or install an nShield HSM. Always consult your company health and safety policy before attempting to lift and carry the module. Two competent persons are required if it is necessary to lift the module to a level above head height (for example, during installation in a rack or when placing the module on a high shelf).

2.1.4. Environmental requirements

To ensure good air flow through and around the module after installation, do not obstruct either the fans and vents at the rear or the vent at the front. Ensure that there is an air gap around the module, and that the rack itself is located in a position with good air flow.

2.1.4.1. Temperature and humidity recommendations

Entrust recommends that your module operates within the following environmental conditions.

Environmental conditions	Operating range (Min. | Max.)		Comments
Operating temperature	5 °C	35 °C	-
Storage temperature	-20 °C	70 °C	-
Operating humidity	10 %	85 %	Relative. Non-condensing at 35 °C.

Environmental conditions	Operating range (Min. | Max.)		Comments
Storage humidity	0 %	95 %	Relative. Non-condensing at 35 °C.
Altitude	-100 m	2000 m	Above Mean Sea Level (AMSL)

2.1.4.2. Cooling requirements

Adequate cooling of your module is essential for trouble-free operation and a long operational life. During operation, you can use the `stattree` utility supplied with the Security World Software to check the actual and maximum temperature of the module. You are advised to do this directly after installing the unit in its normal working environment. Monitor the temperature of the unit over its first few days of operation. You can run the utility from a client machine that has the Security World software installed and has the HSM enrolled to it.

In the unlikely event that the internal encryption module overheats, the module shuts down (see Module Overheating). If the whole nShield HSM overheats, the warning LED on the front panel illuminates with an orange color (see Orange warning LED) and a critical error message is shown on the display.

2.1.5. 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.

2.2. Install a network-attached HSM into a rack

This guide covers the following HSMs:

- nShield Connect
- nShield 5c

- nShield 5c 10G

Always handle modules correctly. Take due account of the weight and dimensions of the HSM when selecting a location for storage or installation. For more information, see Handling an HSM.

You cannot install or configure the HSM remotely.

To install the HSM in a 19" rack, follow the instructions supplied with your rack mounting kit.

To install the HSM in a cabinet or a shelf, fit self-adhesive rubber feet to the bottom of the HSM, one in each corner.

If you encounter any problems during the install process, refer to Troubleshooting. This page includes explanations for the status LED, log messages, and audible warnings as well as other information.

2.2.1. Connecting Ethernet, console and power cables

The connectors for Ethernet cables and mains power cables are at the rear of the HSM.

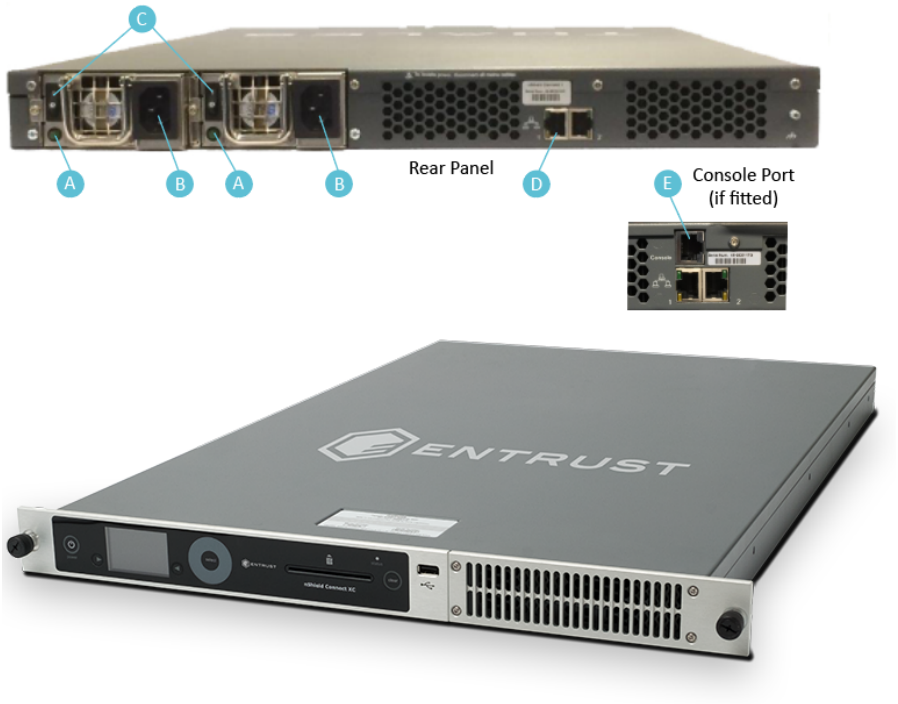
Ensure that:

- All power cables are routed to avoid sharp bends, hot surfaces, pinches, and abrasion.
- You connect mains power cables to **both** the PSUs.
- The rocker switch for each PSU is in the **on** position.

2.2.1.1. nShield Connect and nShield 5c

The HSM is an Ethernet network device capable of supporting up to 100m of Ethernet cable. You must use a CAT5e UTP cable or better when connecting the HSM to a 100Mbit or 1Gbit Ethernet device. You must use a CAT3 cable or better for 10Mbit connections.

The following image shows the Ethernet, console and mains power connections:



Key	Description
A	Green LED if on, confirms power is on and unit is not in Standby mode
B	Mains power connection
C	Rocker switch to turn PSU on and off
D	Ethernet port. Two Ethernet ports are available. Port 1 is the left-hand connector when the HSM is viewed from the back
E	RJ45 port for a serial console cable

If you connect only one network cable to the HSM, connect it to network port 1. This is the left-hand Ethernet connector on the rear of the HSM (shaded in the image).

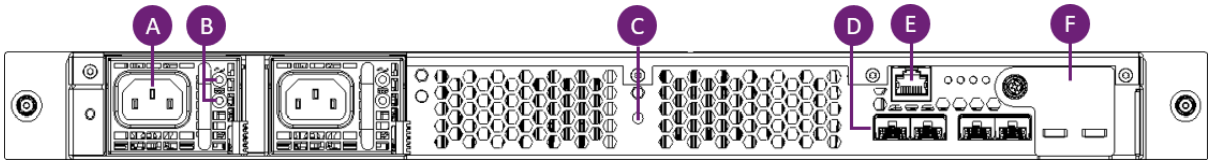
If the green LED is on, the PSU is operational and receiving power, and is not in Standby mode. If a power cable is not fitted correctly, or a rocker switch is not turned on, an audible warning is given and the orange warning LED on the front panel is turned on.

For more information:

- Audible warnings, see Audible warning.
- The orange warning LED, see Orange warning LED.
- Identifying and replacing a faulty PSU, see the *HSM Power Supply Unit Installation Sheet*.

2.2.1.2. nShield 5c 10G

The HSM is an Ethernet network device. The cable lengths and speeds it will support depend on the SFP+ transceivers used. Entrust recommends you use the SFP+ modules detailed in SFP+ transceivers and refer to the manufacturer documentation for the interconnection and physical layer specifications. These modules have been qualified for use with the nShield 5c 10G.



Key	Description
A	Mains power connection
B	Two dual-colour status LEDs for the mains power connection. They are steady green in normal operation and amber or blinking green for various fault conditions. • top LED: AC power-in • bottom LED: DC power-out
C	Diagnostic LED
D	4 SFP+ 10G ports Plug the SFP+ transceiver into the port before you connect the ethernet cable. If you connect only one Ethernet cable to the HSM, Entrust recommends that you connect it to an SFP transceiver in port 1. For more information on SFP transceivers, see SFP+ transceivers.
E	RJ45 port for a serial console cable
F	Battery module Do not remove the battery module for longer than 15 minutes at a time. See nShield 5c 10G maintenance.

2.2.1.3. nShield 5c 10G network profiles

The nShield 5c 10G has four ports that accept pluggable transceivers and offer copper or fiber connectivity. This enables port-based separation of different types of network traffic: Ports 1 and 2 (`eno1` and `eno2`) are management interfaces, ports 3 and 4 (`eno3` and `eno4`) are the data interfaces. It isolates management services (traffic to and from the platform) from the cryptography services (traffic to and from a tenant). Previous HSM models, such as Connect XC and 5c support separate IP configurations but do not offer traffic separation.

You can set the network profile of the 5c 10G to one of the following configurations:

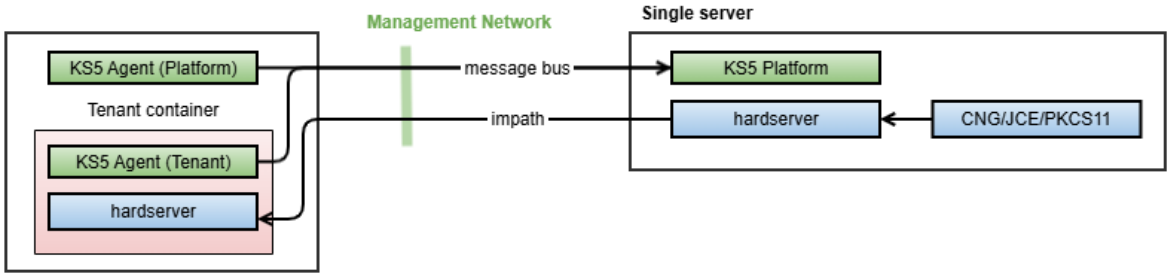
Profile	eno1	eno2	eno3	eno4
Single port (default)	Mgmt + Data	-	-	-
Bonded ports	Mgmt + Data, bonded		-	-
Separated ports	Mgmt	-	Data	-
Separated and bonded ports	Mgmt, bonded		Data, bonded	

You can manage the profile types using KeySafe 5 or through the serial CLI.

- On the serial CLI, you can give the **single** profile a static IPv4 or IPv6 configuration. Other profiles or pairs of ports can then be configured using KeySafe 5.
- In all profiles the default configuration enables DHCPv4 and SLAAC.
- In the **bonded** and **separated and bonded** profiles, pairs of interfaces can be bonded together using either active backup or 802.3ad bonding modes. The configuration of each bonding is independent.

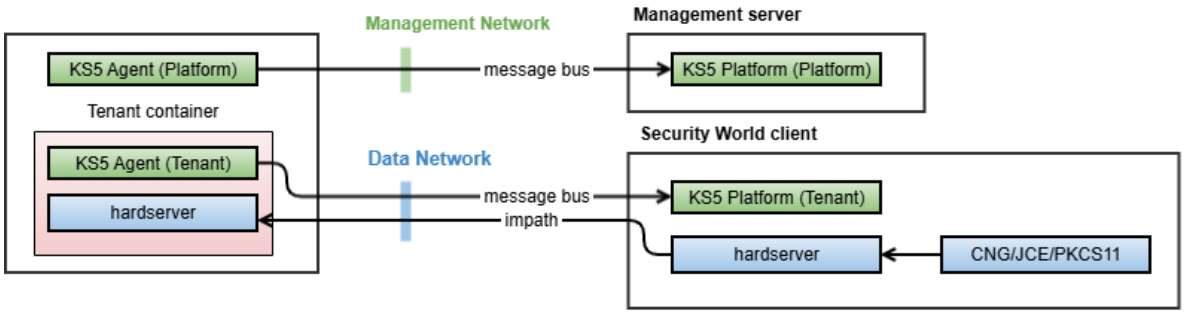
To see what settings are user-configurable, see nShield HSM configuration files.

Example: Non-separated profile



This is a simple deployment with non-separated network traffic, using either the **single port** or **bonded ports** profiles. All device management operations and security world operations are performed within the single KeySafe 5 server. The single server is also running the hardserver and the existing CSPs (PKCS11/JCE/CNG) but either component can be deployed on separate systems that are routable from the 5c 10G's management interfaces.

Example: Separated profile



This is network port-level service separation, using either the **separated ports** or **separated and bonded ports** profiles.

- Device management is performed through the management network, using one instance of the KeySafe 5 server. This is where all network configuration, system logging, and configuration of tenants is performed.
- Security world management and crypto operations are performed on the data network, directly on the security world client and in the tenant KeySafe 5 instance.

2.2.2. Connecting the Serial Console

On supported HSM hardware variants (see Model numbers) there is a serial console port that provides access to a serial console command line interface that enables remote configuration of the HSM.

The Serial console port is always available on the nShield 5c 10G.

The RJ45 connector for the serial cable is at the rear of the HSM and is labelled Console, see Connecting Ethernet, console and power cables. The connector can be directly connected to your client machine or connected to a serial port aggregator for remote access. For a specification of the serial cable required, see Serial Console cable pinout information. The serial port will operate at 115200 baud, 8 data bits, no parity, and 1 stop bit (115200/8-N-1).

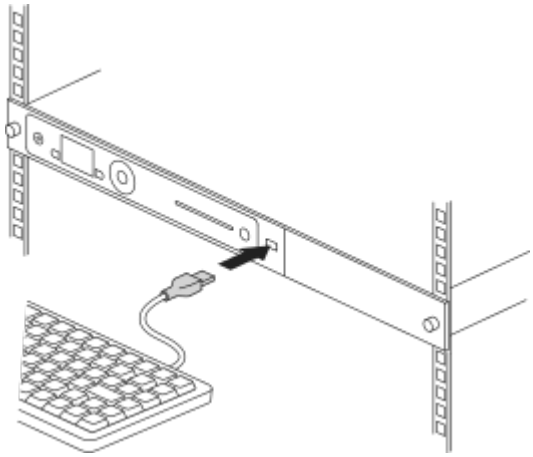
2.2.2.1. Serial Console cable pinout information

The pinout information for the RJ-45 to DB-9 cable to be used to access the HSM Serial Console is provided in the table below:

Signal	Console Port (DTE) RJ-45 Pin	Adapter DB-9 Pin	Signal
CTS	1	7	RTS

Signal	Console Port (DTE) RJ-45 Pin	Adapter DB-9 Pin	Signal
DTR	2	4	DSR
TxD	3	3	RxD
GND	4	5	GND
GND	5	5	GND
RxD	6	2	TxD
DSR	7	6	DTR
RTS	8	8	CTS

2.2.3. Connecting the optional USB keyboard (nShield Connect and nShield 5c)



Instead of using the controls on the front panel to configure the HSM, you can use a US or UK keyboard. You might find a keyboard easier for entering dates and IP addresses. You connect the keyboard to the USB connector on the front of the HSM.

2.2.3.1. Configuring an HSM for your keyboard type

To configure an HSM for your keyboard type, select **System > System configuration > Keyboard layout** and then choose the keyboard type you require.

When you have connected a keyboard and configured the HSM for its use, you can enter numbers and characters directly into the display. See Using a keyboard to control the unit for more about using a keyboard and keystroke shortcuts.

2.2.4. Checking the installation

Ensure that:

- The HSM is safely and securely installed.
- The mains cables and Ethernet cable are securely fitted.
- The HSM powers up successfully when you turn on the power supply at the rear of the HSM.

3. nShield PCIe HSMs

3.1. Prerequisites and product information

This guide covers the following HSMs:

- nShield Solo
- nShield Solo XC
- nShield 5s

These Hardware Security Modules (HSMs) are for use in servers and appliances.

- For further information about the HSM and HSMs in general, see nShield v13.6.16 HSM User Guide.
- For help installing the Security World software, see nShield Security World Software v13.6.16 Installation Guide.
- For guidance on using your HSM and the Security World software, see nShield Security World v13.6.16 Management Guide.
- For further information about compatible operating systems and virtual environments, see Compatibility in the release notes for the version of Security World you are using.

See Model numbers for a list of PCIe HSMs and their model numbers.

3.1.1. Power and safety requirements

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

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

The HSMs are 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.

3.1.2. Handling the HSM

nShield HSMs contain 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.

3.1.3. Environmental requirements

The nShield HSMs operate within the following environmental conditions.

3.1.3.1. Temperature and humidity specifications

nShield 5s

nShield 5s environmental conditions	Operating range		Comments
	Min.	Max.	
Operating temperature*	5°C (41°F)	55°C (131°F)	Subject to sufficient airflow
Storage temperature	-5°C (-23°F)	60°C (140°F)	-
Transportation temperature	-40°C (-40°F)	70°C (158°F)	-
Operating humidity	5%	85%	Relative. Non-condensing at 30°C (86°F)
Storage humidity	5%	93%	Relative. Non-condensing at 30°C (86°F)
Transportation humidity	5%	93%	Relative. Non-condensing at 30°C (86°F)
Altitude	-100m (-328ft)	2000m (6561ft)	Above Mean Sea Level

*Air temperature at PCIe card inlet surface. For more information, see Cooling requirements.

nShield Solo

nShield Solo environmental conditions	Operating range		Comments
	Min.	Max.	
Operating temperature*	10°C (50°F)	35°C (95°F)	Subject to sufficient airflow
Storage temperature	-20°C (-4°F)	70°C (158°F)	-
Operating humidity	10%	90%	Relative. Non-condensing at 35°C (95°F)
Storage humidity	0	85%	Relative. Non-condensing at 35°C (95°F)

*Air temperature at PCIe card inlet surface. For more information, see Cooling requirements.

nShield Solo XC

nShield Solo XC environmental conditions	Operating range		Comments
	Min.	Max.	
Operating temperature	5°C (41°F)	55°C (131°F)	Subject to sufficient airflow
Storage temperature	-5°C (-23°F)	60°C (140°F)	-
Transportation temperature	-40°C (-40°F)	70°C (158°F)	-
Operating humidity	5%	85%	Relative. Non-condensing at 30°C (86°F)
Storage humidity	5%	93%	Relative. Non-condensing at 30°C (86°F)
Transportation humidity	5%	93%	Relative. Non-condensing at 30°C (86°F)
Altitude	-100m (-328ft)	2000m (6561ft)	Above Mean Sea Level

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.

3.1.3.2. Cooling requirements

An air velocity of 1.9 m/s (373 LFM) is recommended for a module in operation.

During installation, ensure there is adequate airflow around the module. Airflow from fans must be directed to the inlet surface of the module such that air is flowing through and across the length of the module. To maximize airflow, use a PCIe slot with no neighboring modules if possible. If airflow is limited, consider fitting extra cooling fans.

The nShield Solo (non-XC variant) and 5s HSMs are passively cooled PCIe cards that require the host to provide sufficient airflow for cooling. Passive cards should not be powered without cooling airflow in place.

Ensure the module has adequate cooling. Failure to do so can result in damage to the module or computer.

To check the actual and maximum temperature of the module during operation, see Maintenance of nShield Hardware. 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.

3.1.3.3. Cooling recommendations for a desktop installation

For a desktop installation running in operating environmental conditions, dedicated airflow is required across the module. If the system cannot provide the necessary airflow, Entrust recommends you add a sufficiently powerful dedicated fan to directly cool the module. For details regarding the cooling requirements see Cooling requirements.

3.1.3.4. Cooling recommendations for a server installation

The desktop cooling recommendations further apply to a server installation. In addition, power and airflow control software is sometimes available in a server installation. If this is the case, Entrust recommends you:

- Configure the target air velocity in the software to ensure it does not fall below the airflow recommendations of the module. For details regarding the cooling requirements, see Cooling requirements.
- Ensure that the PCIe slot has been configured to fulfil the module power requirements.

3.1.4. 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.

3.2. Install a PCIe HSM

This guide covers the following HSMs:

- nShield Solo XC
- nShield 5s

If you encounter any problems during the install process, refer to HSM Status indicators (nShield Solo and Solo XC) and Morse code error messages (nShield Solo and Solo XC), or HSM status indicators and error codes (nShield 5s). These pages explain the status LED messages, and provide other information.

3.2.1. Module pre-installation steps

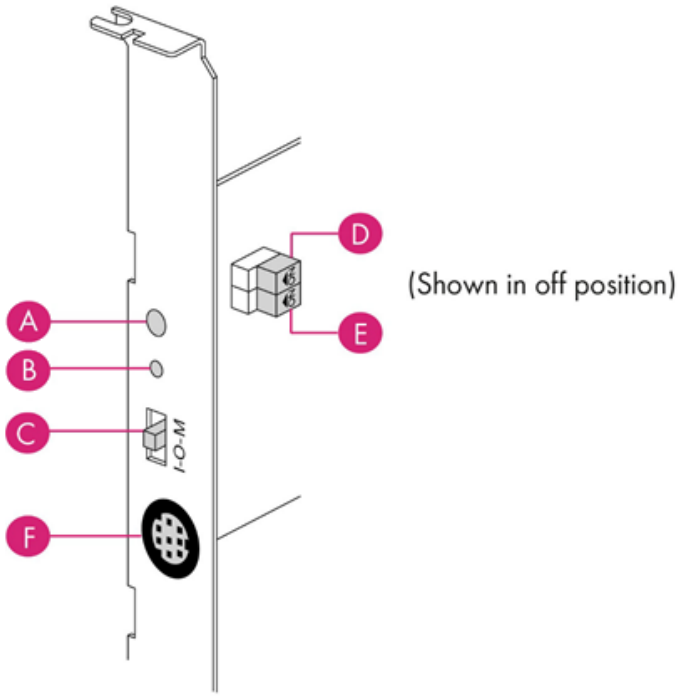
Check the module to ensure that there is no sign of damage or tampering:

- Check the epoxy resin security coating, or the metal lid for the Solo XC, for obvious signs of damage.
- 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.
- **nShield Solo and Solo XC:** Check that the physical switches are in the required positions. See the diagram in the *Module back panel* section for switch labelling.
    - To use the remote mode switch override to change the mode, the physical mode switch (**C**) must be set to Operational (**O**).
    - To use the Remote Administration feature 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**).

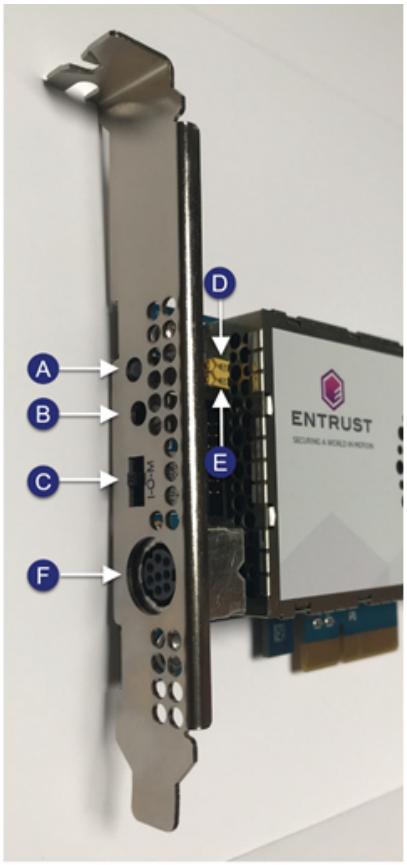
The default factory setting of the jumper DIP switch **E** is **Off**. This enables remote MOI switching. Factory shipping nShield Solo HSMs loaded with firmware 2.61.2 or greater will support remote MOI switching by default. Customers who expressly do not want to enable the remote MOI switching capability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

- To deactivate the physical mode switch (**C**), change jumper switch **D** to the **On** position.

3.2.1.1. Module back panel



nShield Solo



nShield Solo XC

Label	Description
A	Status LED
B	Recessed clear button (Solo and Solo XC) or recovery mode button (5s)
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 Checking and changing the mode on an nShield Solo module for more information.

Label	Description
E	Remote mode override jumper switch, in the **Off** position. When set to **On**, remote mode switching is disabled. See Checking and changing the mode on an nShield Solo module 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. The nShield 5s does not contain physical switches.

3.2.2. Swap the module bracket

If the fitted module bracket is not the same height as the slot, swap it for the correct size. 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 electrostatic discharge (ESD) precautions.

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.

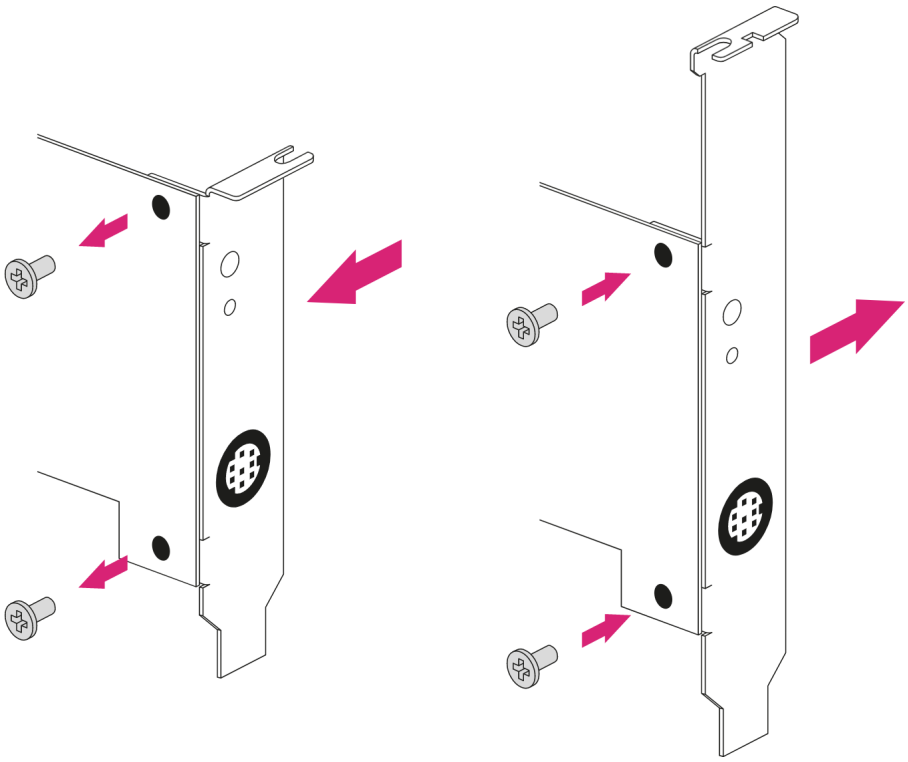


Figure 1. Screw placement on an nShield 5s.

Screw placement is the same on a Solo module bracket, however the Solo and Solo XC brackets also have a physical mode switch.

3.2.3. Install the module

1. Power off the system and while taking electrostatic discharge 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.

   You must only install the HSM into a PCIe x4 slot, unless you are installing an nShield Solo (non-XC variant), which can use a PCIe x1 slot. See the instructions that your computer manufacturer supplied to correctly identify the slots on your computer.

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 XC only**) Check that the two jumper switches on the module are still in required positions (see Back panel and jumper switches).
7. (**Solo XC only**) Check that the mode switch is still in the center **O** (operational) position.
8. Replace the computer case.

3.2.4. 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.

3.2.5. After installing the module

3.2.5.1. Set the system clock nShield 5s only

Set the system clock. See Setting the system clock.

3.2.5.2. Install the nShield World software

If the Security World software has not already been installed, you must install the Security World Software by following the instructions in the nShield Security World Software v13.6.16 Installation Guide.

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.

nShield 5s only

If this is not the first HSM installed in this host, the Security World software is already installed. However, you still need to set up communication between the host and the newly installed module. The module must either be in factory state or have been previously prepared for use on this host. For more information, see Set up communication between host and module (nShield 5s HSMs).

If the new module has been supplied from the factory it will already be in factory state.

4. nShield USB HSMs

4.1. Prerequisites and product information

This guide covers the following HSMs:

- nShield Edge

This 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 certifi cate 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.

- For further information about the HSM and HSMs in general, see nShield v13.6.16 HSM User Guide.
- For help installing the Security World software, see nShield Security World Software v13.6.16 Installation Guide.
- For guidance on using your HSM and the Security World software, see nShield Security World v13.6.16 Management Guide.
- For further information about compatible operating systems and virtual environments, see Compatibility in the release notes for the version of Security World you are using.

See Model numbers for a list of portable (USB) HSMs and their model numbers.

4.1.1. Safety and security

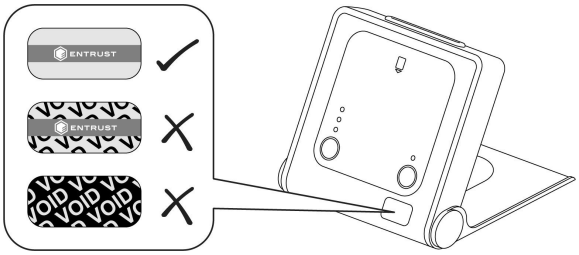
Do not connect the HSM to a computer that does not have the Security World software installed on it.

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

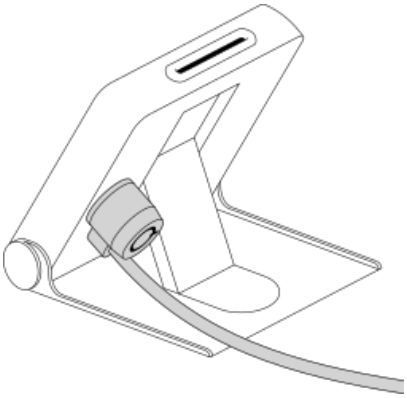
> void.

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.

4.1.2. 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.

4.1.3. Dimensions and operating conditions

Dimensions (with stand closed)	**120 (w) x 118 (h) x 27 (d) mm**
Weight	340g

Dimensions (with stand closed)	**120 (w) x 118 (h) x 27 (d) mm**
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

4.1.4. 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.

4.2. Set up the nShield Edge

If you encounter any problems during the setup process, refer to Troubleshooting.

4.2.1. 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

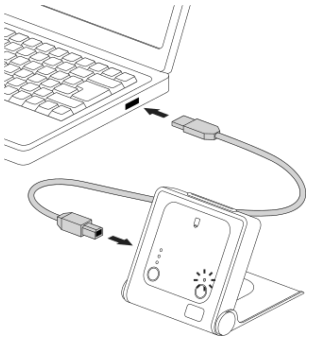
Set power options to never put computer to sleep.

4.2.2. Connecting an nShield Edge

Do the following:

4.2.2.1. 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**.

4.2.2.2. 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 hard-server. 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. Creating a Security World involves putting the nShield Edge into Initialization (I) mode. See Changing the mode for more information.

4.2.3. 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 Optional features, or follow the instructions supplied with the certificate or Activator card.

4.2.4. 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.

4.2.5. 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.