ENTRUST

nShield Security World

nShield Solo and Solo XC v12.50.4 Installation Guide

4 March 2024

Contents

1 Introduction

The nShield® Solo and Solo XC are Hardware Security Modules (HSM) for servers and appliances.

1.1 About this guide

This guide includes:

- Installing the nShield Solo and nShield Solo XC. See *Installing the module* on page 33.
- Installing the Security World Software. See *Installing the software* on page 39.
- Steps to check the installation. See *Checking the installation* on page 47.
- A description of the module status indicators. See *Status indicators* on page 53.
- Instructions about removing existing software. See *Uninstalling existing software* on page 54.

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 and nShield Solo XC.

For information on integrating nCipher products with third-party enterprise applications, see https://www.ncipher.com.

1.1.1 Model Numbers

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

Model number	Used for
xC3*xxx*E-*xxx* xC4*xxx*E-xxx	nCipher nShield Solo PCIe
xC30*x*5E-*xxx* xC40*x*5E-*xxx*	nCipher nShield Solo XC PCIe

1.2 Additional documentation

You can find additional documentation in the **`document`** 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* .

See the *User Guide* for a glossary of terms.

nCipher strongly recommends that you read the release notes in the **`release`** directory of your installation disc before you use the module. These notes contain the latest information about your product.

1.2.1 Terminology

The nShield Solo and nShield Solo XC are referred to as the *nShield Solo* and *nShield Solo XC*, the *hardware security module*, or the *HSM* in this guide.

1.3 Typographical conventions

ℹ The word **Note** indicates important supplementary information.

Pay particular attention to any warnings and cautions accompanied by the following symbols:

⚠	⚠	⚠	⚠
Risk of electric shock to the user	Risk of damage to the module	Risk of static damage to the module	Risk of losing critical security parameters

2 Hardware security modules

2.1 Power requirements

Module	Maximum power
Solo	9.9W
Solo XC	24W

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

The Solo and Solo XC modules 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.

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 connector 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* on page 11.

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 Solo and Solo XC modules are designed to operate in moderate climates only. Never operate the modules in dusty, damp, or excessively hot conditions.
Never install, store, or operate the Solo and Solo XC modules 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, it stops operating and displays the **SOS-T** error message on the Status LED (see *Status indicators* on page 53).

2.6 Physical location considerations

nCipher 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.

Modules de sécurité du matériel informatique

2.7 Besoins en énergie

Module	Puissance maximale
Solo	9.9W
Solo XC	24W

Remarque: Assurez-vous que l'alimentation électrique de votre ordinateur est suffisamment élevée pour fournir l'énergie électrique requise.

Le Solo et les cartes Solo XC sont conçus pour être installés sur un ordinateur ou un serveur personnel certifié, ou un équipement similaire.

Si votre ordinateur peut fournir l'énergie électrique requise et un refroidissement suffisant, vous pouvez installer de multiples modules sur votre ordinateur.

2.8 Manipulation des modules

Le module contient des dispositifs à semi-conducteurs capables de supporter des conditions normales de manutention. Toutefois, ne faites pas tomber le module et ne l'exposez pas à des vibrations excessives.

Avant d'installer le matériel informatique vous devez déconnecter votre ordinateur de sa source d'alimentation électrique. Assurez-vous qu'il reste un contact à la terre. Procédez à l'installation avec soin et suivez toutes les instructions de sécurité de ce guide et du constructeur de votre ordinateur.

Les décharges d'électricité statique peuvent endommager les modules. Ne touchez pas les tiges de connexion du PCIe, ni la zone exposée du module.

Laissez le module dans son sac antistatique jusqu'au moment de l'installation. Portez toujours une dragonne antistatique reliée à un objet en métal mis à la terre. Vous devez aussi vous assurer que le châssis de l'ordinateur est mis à la terre lorsque vous installez ou retirez un module interne.

2.9 Exigences environnementales

Lorsque vous installez le module, assurez-vous que l'air circule bien autour. Pour maximiser le débit d'air, utilisez un connecteur de PCIe qui ne comporte aucun module à proximité si possible. Si le débit d'air est limité, vous pouvez envisager le montage de ventilateurs supplémentaires sur le boîtier de votre ordinateur.

⚠ Une ventilation insuffisante peut endommager le module ou l'ordinateur dans lequel le module est inséré.

Manipulez toujours le module correctement. Pour plus d'informations, reportez-vous à *Manipulation des modules* on page 14.

2.10 Température et taux d'humidité recommandés

Nous vous recommandons de faire fonctionner le module Solo dans les conditions environnementales suivantes.

Conditions environnementales Solo	Plage de fonctionnement		Commentaires
	Min.	Max.	
Température ambiante de fonctionnement	10°C	35°C	Avec un débit d'air suffisant
Température de stockage	-20°C	70°C	-
Taux d'humidité de fonctionnement	10%	90%	Relative. Non condensation à 35 °C
Taux d’humidité de stockage	0	85%	Relative. Non condensation à 35 °C

Nous recommandons de faire fonctionner le module Solo XC dans les conditions environnementales suivantes.

Conditions environnementales Solo XC	Plage de fonctionnement		Commentaires
	Min.	Max.	
Température ambiante de fonctionnement	5°C	55°C	-
Température de stockage	-5°C	60°C	-
Température de transport	-40°C	70°C	-
Taux d'humidité de fonctionnement	5%	85%	Relative. Non condensation à 30 °C
Taux d’humidité de stockage	5%	93%	Relative. Non condensation à 30 °C
Taux d'humidité de transport	5%	93%	Relative. Non condensation à 30 °C

⚠ Le Solo et les modules Solo XC sont conçus pour fonctionner dans des climats tempérés uniquement. N'utilisez jamais les modules dans un environnement poussiéreux, humide ou excessivement chaud. N'installez jamais, ne stockez jamais et n'utilisez jamais le Solo et les modules Solo XC dans des endroits où ils pourraient recevoir des gouttes ou des éclaboussures.

2.11 Besoins de refroidissements

Le refroidissement adéquat du module est essentiel pour un fonctionnement sans problèmes et une longue durée de fonctionnement. Lors du fonctionnement vous pouvez utiliser l'outil stattree fourni pour vérifier la température réelle et maximum du module. Il est conseillé de faire cela directement après l'installation du module dans son environnement de fonctionnement normal. Contrôlez la température du module au cours des premiers jours de fonctionnement. Si le module dépasse la température de fonctionnement de sécurité, il cesse de fonctionner et affiche le message d'erreur SOS-T sur le voyant d'état à DEL (voir *Status indicators* on page 53).

2.12 Remarques concernant l'emplacement physique

Les HSM de nCipher nShield sont certifiés au niveau 2 et 3 de NIST FIPS 140. En plus de la protection intrinsèque fournie par un HSM nShield, les clients doivent faire preuve d'une grande application pour s'assurer que l'environnement dans lequel les HSM nShield sont déployés est configuré correctement et est régulièrement examiné dans le cadre d'un programme complet de réduction des risques pour évaluer à la fois les menaces logiques et les menaces physiques. Les applications qui fonctionnent dans cet environnement devront être authentifiées pour s'assurer de leur légitimité et pour contrecarrer la prolifération éventuelle de logiciels malveillants susceptibles de les infiltrer tandis qu'elles accèdent aux services de cryptographie des HSM. L'environnement déployé doit adopter des mesures de «défense en profondeur » et soigneusement envisager l'emplacement physique pour empêcher la détection d'émanations électromagnétiques qui pourraient autrement révéler par inadvertance un contenu cryptographique.

Hardware-Sicherheitsmodule

2.13 Spannungsversorgung

Modul	Maximale Leistung
Solo	9.9W
Solo XC	24W

Hinweis: Stellen Sie sicher, dass die Spannungsversorgung Ihres Computers so ausgelegt ist, dass sie die erforderliche Leistung bereitstellen kann.

Die Solo und Solo XC-Karten dienen der Installation in einem zertifizierten PC, Server oder einem anderen ähnlichen Gerät.

Wenn Ihr Computer die erforderliche Leistung und eine ausreichende Kühlung bereitstellen kann, können in einem Computer auch mehrere Module installiert werden.

2.14 Umgang mit Modulen

Das Modul besteht aus Festkörpergeräten, die einer normalen Behandlung standhalten. Achtung: Lassen Sie das Modul nicht fallen oder setzen Sie es übermäßigen Vibrationen aus.

⚠ Vor Installation der Hardware müssen Sie Ihren Computer von der Spannungsversorgung trennen. Stellen Sie sicher, dass ein masseführender (geerdeter) Kontakt bestehen bleibt. Führen Sie die Installation sorgfältig aus und befolgen Sie alle Sicherheitsanweisungen in dieser Anweisung und den Anweisungen Ihres Computerherstellers.

⚠ Statische Entladungen können zu Beschädigungen an den Modulen führen. Berühren Sie niemals die Steckerstifte des PCIe oder den freiliegenden Bereich des Moduls.

Bewahren Sie das Modul bis zum Beginn der Installation in seinem antistatischen Beutel auf. Tragen Sie immer Erdungsarmbänder, die mit einem masseführenden Metallgegenstand verbunden sind. Stellen Sie sicher, dass der Rahmen des Computers mit einem Masseleiter verbunden ist, während Sie ein Modul installieren oder entfernen.

2.15 Umweltanforderungen

Stellen Sie bei der Installation des Moduls sicher, dass der Bereich um das Modul gut belüftet ist. Um eine optimale Belüftung bereitzustellen, verwenden Sie nach Möglichkeit einen PCIe-Slot ohne benachbarte Module. Sollte eine optimale Belüftung nur begrenzt möglich sein, sollten Sie im Computergehäuse zusätzliche Kühlgebläse installieren.

⚠ Wenn das Modul nicht ausreichend gekühlt wird, können das Modul wie auch der Computer, in dem das Modul verbaut ist, beschädigt werden.

Installieren und behandeln Sie das Modul stets vorschriftsgemäß. Weitere Informationen finden Sie *Umgang mit Modulen* on page 17.

2.16 Empfohlene Temperatur- und Feuchtigkeitswerte

Wir empfehlen, das PCIe-Modul innerhalb der folgenden Umgebungsbedingungen zu betreiben.

Umgebungsbedingungen Solo	Betriebsbereich		Anmerkungen
	Min.	Max.	
Betriebstemperaturumgebung	10°C	35°C	Ausreichend gute Belüftung erforderlich
Temperatur Lagerung	-20°C	70°C	-
Betriebsfeuchtigkeit	10%	90%	Relativ. Nicht kondensierend bei 35°C
Feuchtigkeit Lagerung	0	85%	Relativ. Nicht kondensierend bei 35°C

Wir empfehlen, das Solo XC-Modul innerhalb der folgenden Umgebungsbedingungen zu betreiben.

Umgebungsbedingungen Solo XC	Betriebsbereich		Anmerkungen
	Min.	Max.	
Betriebstemperaturumgebung	5°C	55°C	-
Temperatur Lagerung	-5°C	60°C	-
Temperatur Transport	-40°C	70°C	-
Betriebsfeuchtigkeit	5%	85%	Relativ. Nicht kondensierend bei 30°C
Feuchtigkeit Lagerung	5%	93%	Relativ. Nicht kondensierend bei 30°C
Feuchtigkeit Transport	5%	93%	Relativ. Nicht kondensierend bei 30°C

⚠ Die Solo- und Solo XC-Module dürfen ausschließlich in gemäßigten Klimabedingungen betrieben werden. Betreiben Sie die Module niemals unter staubigen, feuchten oder übermäßig heißen Bedingungen.Installieren, lagern oder betreiben Sie die Solo- und Solo XC-Module niemals an Orten, wo sie tropfenden oder spritzenden Flüssigkeiten ausgesetzt sind.

2.17 Anforderungen Kühlung

Für einen störungsfreien Betrieb und eine lange Lebensdauer des Moduls ist eine ausreichende Kühlung wesentlich.

Während des Betriebs können Sie das im Lieferumfang enthaltene stattree-Programm nutzen, um die tatsächliche und maximale Temperatur des Moduls zu überprüfen. Es wird empfohlen, die Temperatur des Moduls direkt nach der Installation in dessen tatsächlicher Arbeitsumgebung zu messen. Überwachen Sie die Temperatur des Moduls in den ersten Tagen des Betriebs. Sollte die Betriebstemperatur des Moduls den sicheren Bereich übersteigen, unterbricht es den Betrieb und die Status-LED zeigt die Fehlermeldung „SOS-T error“ an (siehe *Status indicators* on page 53).

2.18 Hinweise zum physischen Standort

Die nShield-Module (HSM) von nCipher sind gemäß NIST FIPS 140-2 Level 2 und 3 zertifiziert. Zusätzlich zum Eigenschutz, der durch ein nShield-HSM bereitgestellt wird, müssen Kunden das Modul vorsichtig verwenden und sicherstellen, dass die Umgebung, in der das nShield-Modul genutzt wird, ordnungsgemäß konfiguriert ist und regelmäßig im Rahmen eines umfassenden Programms zu Risikominimierung überprüft wird (um sowohl logische als auch physische Gefahren zu bewerten). Anwendungen, die in der Umgebung genutzt werden, müssen authentifiziert werden, um a) deren Legitimität sicherzustellen und b) eine mögliche Verbreitung von Malware zu verhindern, die die Umgebung durch Zugriff auf die Verschlüsselungsdienste der HSMe infiltrieren könnte. Die genutzte Umgebung muss über gestaffelte Sicherheitsmaßnahmen (defense in depth) geschützt sein und der physische Standort muss sorgfältig ausgewählt werden, um eine Erkennung elektromagnetischer Strahlungen zu vermeiden, die unbeabsichtigt Verschlüsselungsinformationen preisgeben könnten.

Módulos de Seguridad de Hardware

2.19 Requerimientos de corriente eléctrica

Módulo	Potencia máxima
Solo	9.9W
Solo XC	24W

Nota: Asegúrese de que la fuente de alimentación de su computadora haya sido clasificada para suministrar la potencia eléctrica requerida.

Las tarjetas Solo y Solo XC están diseñadas para ser instaladas en una computadora personal, servidor o equipo similar certificados.

Si su computadora puede suministrar la energía eléctrica y disipación de calor suficientes, puede instalar varios módulos en su computadora.

2.20 Manipulación de módulos

El módulo contiene dispositivos de estado sólido que pueden soportar una manipulación normal. Sin embargo, no deje caer el módulo ni lo exponga a vibraciones excesivas.

Antes de instalar el hardware debe desconectar su computadora de la fuente de energía. Asegúrese de que cuente con conexión a tierra. Realice la instalación con cuidado y siga todas las instrucciones de seguridad en esta guía y las indicadas por el fabricante de su computadora.

Los módulos pueden dañarse por cargas estáticas. No toque los pines del conector PCIe ni el área expuesta del módulo.

Deje el módulo en su bolsa antiestática hasta que esté listo para instalar. Siempre utilice una muñequera antiestática conectada a un objeto metálico que haga tierra. Debe asegurarse de que el marco de la computadora esté haciendo tierra cuando instala o retira un módulo interno.

2.21 Requerimientos ambientales

Cuando instale el módulo, asegúrese de que haya un buen flujo de aire alrededor del mismo. Para maximizar el flujo de aire, utilice una ranura de PCIe que no esté adyacente a otros módulos, de ser posible. Si el flujo de aire es limitado, considere instalar ventiladores adicionales en la torre de su computadora.

No proveer ventilación adecuada puede resultar en daños al módulo o a la computadora en la que se instaló el módulo.

Siempre manipule el módulo correctamente. Por más información, vea *Manipulación de módulos* on page 20.

2.22 Recomendaciones de temperatura y humedad

Recomendamos que el Solo opere dentro de las siguientes condiciones ambientales.

Condiciones ambientales para Solo	Rango de operación		Comentarios
	Min.	Max.	
Temperatura ambiente de operación	10°C	35°C	Sujeto a flujo de aire suficiente
Temperatura de almacenamiento	-20°C	70°C	-
Humedad de operación	10%	90%	Relativa. Sin condensación a los 35°C
Humedad de almacenamiento	0	85%	Relativa. Sin condensación a los 35°C

Recomendamos que el módulo Solo XC opere dentro de las siguientes condiciones ambientales.

Condiciones ambientales para Solo XC	Rango de operación		Comentarios
	Min.	Max.	
Temperatura ambiente de operación	5°C	55°C	-
Temperatura de almacenamiento	-5°C	60°C	-
Temperatura de transporte	-40°C	70°C	-
Humedad de operación	5%	85%	Relativa. Sin condensación a los 30°C
Humedad de almacenamiento	5%	93%	Relativa. Sin condensación a los 30°C
Humedad de transporte	5%	93%	Relativa. Sin condensación a los 30°C

⚠ Los módulos Solo y Solo XC están diseñados para operar solamente en climas moderados. Nunca opere estos módulos en condiciones de mucho polvo, humedad o excesivamente calurosas. Nunca instale, almacene u opere los módulos Solo y Solo XC en lugares en los que puedan estar sujetos a goteras o salpicaduras de líquidos.

2.23 Requerimientos de ventilación

Para una operación sin problemas y una larga vida de funcionamiento, es esencial que el módulo disponga de una ventilación adecuada.

Durante la operación, puede utilizar la función `stattree` para verificar la temperatura actual y la temperatura máxima del módulo. Se recomienda hacer esto inmediatamente después de instalar el módulo en su ambiente normal de trabajo. Controle la temperatura del módulo durante sus primeros días de operación. Si el módulo excede la temperatura segura de operación, dejará de funcionar y mostrará el mensaje de error `SOS-T` en el LED de estado (ver *Status indicators* on page 53).

2.24 Consideraciones para la ubicación física

Los módulos de seguridad de hardware (HSM) nShield de nCipher están certificados para NIST FIPS 140-2 niveles 2 y 3. Además de la protección intrínseca provista por un HSM nShield, los clientes deben ejercer la diligencia debida para asegurar que el ambiente en el que se instalan los HSM nShield esté configurado apropiadamente y sea evaluado regularmente como parte de un programa exhaustivo de mitigación de riesgos, para evaluar amenazas tanto lógicas como físicas. Las aplicaciones que funcionan en el ambiente pueden ser autentificadas para asegurar su legitimidad y para prevenir cualquier posible proliferación de malware que pudiera infiltrarse cuando accedan a los servicios criptográficos del HSM. EL ambiente desarrollado debe adoptar medidas de "defensa en profundidad" y considerar cuidadosamente la ubicación física que evite la detección de emanaciones electromagnéticas que puedan de otra forma revelar material criptográfico por accidente.

3 Regulatory notices

3.1 FCC class A notice

The nShield Solo and nShield Solo XC HSMs comply with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. The device may not cause harmful interference, and
2. The device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

3.3 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

A Takeback and Recycle program is provided in compliance with the Waste Electrical and Electronic Equipment (WEEE) directive for the recycling of electronic equipment. The program enables you to return an obsolete or surplus nCipher product, which is then disposed of in an environmentally safe manner. For further information or to arrange the safe disposal of your product, e-mail nCipher Support.

Avis juridiques

3.6 Classe A de la FCC

Ce HSM Solo nShield répond aux exigences de la partie 15 du règlement de la FCC. Le fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne peut pas causer d'interférence nuisible, et
2. Cet appareil doit accepter toute interférence reçue, incluant les interférences qui peuvent causer un fonctionnement non désiré.

Cet équipement a été testé et respecte les limites pour les appareils numériques de classe A, selon la partie 15 du règlement de la FCC. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nuisibles lorsque l'équipement fonctionne dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie radio fréquence et, s'il n'est pas installé et utilisé conformément au manuel d'instruction, peut causer des interférences nuisibles à la radiocommunication. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de causer des interférences nuisibles auquel cas l'utilisateur devra corriger les interférences à ses propres frais.

3.7 Certification canadienne - CAN ICES-3 (A)/NMB- 3(A)

3.8 Mises en garde batterie

Danger d'explosion si la batterie n'est pas remplacée correctement. La batterie peut seulement être remplacée par une batterie identique ou du même type. Jetez la batterie usagée conformément à votre réglementation locale d'élimination des déchets.

3.9 Mise en garde substances dangereuses

Ce produit contient une batterie au lithium et d'autres composants électroniques et matériaux qui pourraient contenir des substances dangereuses. Toutefois, ce produit n'est pas dangereux s'il est utilisé correctement.

3.10 Information concernant le recyclage et le traitement

Un programme Take Back et Recycle (Rapportez et Recyclez) est fourni conformément à la directive Waste Electrical and Electronic Equipment (WEEE) pour le recyclage des équipements électroniques. Le programme vous permet de rapporter vos produits nCipher obsolètes ou en excédent, qui seront ensuite traités dans le respect de l'environnement. Pour plus d'informations ou pour organiser le traitement sûr de vos produits, envoyez un courriel à nCipher Support.

Rechtliche Informationen

3.11 Hinweis FCC-Klasse A

Das nShield Solo-HSM erfüllt die Anforderungen von Teil 15 der FCC-Bestimmungen. Der Betrieb des Geräts unterliegt den folgenden zwei Bedingungen:

1. Das Gerät darf keine störenden Interferenzen verursachen, und
2. Dieses Gerät muss störenden Interferenzen, die auf das Gerät auftreffen, widerstehen (einschließlich Interferenzen, die einen ungewollten Betrieb verursachen).

Dieses Gerät wurde gemäß Teil 15 der FCC-Bestimmungen getestet und erfüllt die Grenzwerte für Digitalgeräte der Klasse A. Diese Grenzwerte sollen einen geeigneten Schutz gegen störende Interferenzen bereitstellen, wenn das Gerät in einer industriellen Umgebung betrieben wird. Dieses Gerät erzeugt, nutzt und kann Hochfrequenzenergie ausstrahlen und kann, sofern es nicht gemäß den Anweisungen im Nutzerhandbuch installiert und verwendet wird, Funkverbindungen stören. Der Betrieb dieses Geräts in Wohngegenden kann möglicherweise störende Interferenzen verursachen. In einem solchen Fall muss der Nutzer die Interferenzen auf seine eigenen Kosten abstellen.

3.12 Kanadische Zertifizierung - CAN ICES-3 (A)/NMB- 3(A)

3.13 Batteriebezogende Warnhinweise

Explosionsgefahr, wenn die Batterie nicht korrekt ausgetauscht wird. Die Batterie darf nur gegen den gleichen oder einen gleichwertigen Typ ausgetauscht werden. Entsorgen Sie gebrauchte Batterien gemäß Ihren örtlichen Entsorgungsvorschriften.

3.14 Warnhinweise zu Gefahrenstoffen

Dieses Produkt enthält eine Lithiumbatterie und andere elektronische Komponenten und Materialien, die Gefahrenstoffe enthalten können. Allerdings ist dieses Produkt nicht gefährlich, sofern es bestimmungsgemäß verwendet wird.

3.15 Informationen zu Recycling und Entsorgung

Gemäß der WEEE-Richtlinie (Waste Electrical and Electronic Equipment) wird zur Wiederverwertung von elektronischen Geräten ein Rücknahme- und Recyclingprogramm wird bereitgestellt. Im Rahmen dieses Programms können Sie veraltete oder nicht mehr genutzte nCipher Produkte zurückgeben, die dann umweltfreundlich entsorgt werden. Für weitere Informationen oder um die sichere Entsorgung Ihres Produkts zu veranlassen, senden Sie uns eine E-Mail an nCipher Support.

Notificaciones reglamentarias

3.16 Notificación clase A de la FCC

Este HSM nShield Solo cumple con la parte 1 5 de la reglamentación de la Comisión Federal de Comunicaciones (Federal Communications Commission, FCC) La operación está sujeta a las dos siguientes condiciones:

1. Este dispositivo no debe causar interferencia dañina, y
2. El dispositivo debe aceptar cualquier interferencia recibida, incluyendo aquella que pueda causar operaciones indeseadas.

Este equipo ha sido probado y se ha encontrado que cumple los límites para dispositivos digitales Clase A, según la parte 15 de la reglamentación de la FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias dañinas cuando el equipo opere en un ambiente comercial. Este equipo genera, utiliza y puede emitir energía de radiofrecuencia y, de no ser instalado y utilizado de acuerdo con el manual de instrucciones, puede causar interferencia dañina a las radiocomunicaciones. Es probable que la operación de este equipo en un área residencial cause interferencia dañina, y en este caso el usuario está obligado a remediar la interferencia por sus propios medios.

3.17 Certificación de Canadá - CAN ICES-3 (A)/NMB- 3(A)

3.18 Precauciones por baterías

Peligro de explosión si la batería es colocada incorrectamente. La batería solamente puede ser remplazada por una similar o equivalente. Deseche la batería usada de acuerdo con las instrucciones de desecho locales.

3.19 Precaución por sustancia peligrosa

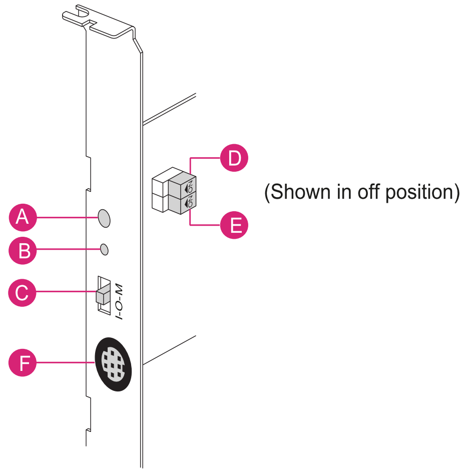
Este producto contiene una batería de litio y otros componentes y materiales electrónicos que pueden contener sustancias peligrosas. Sin embargo, este producto no es peligroso si se utiliza de la manera para cuyo uso fue diseñado.

3.20 Información de desecho y reciclaje

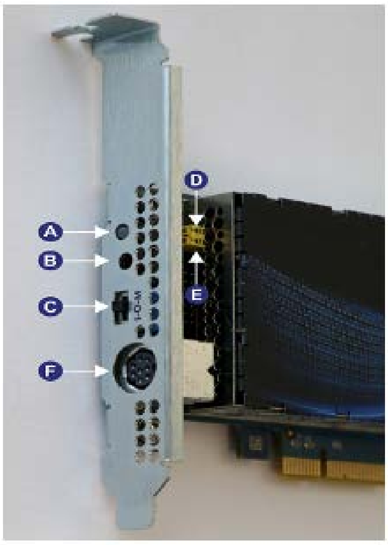
Se proporciona un programa de Devolución y Reciclaje que cumple con la directiva de Residuos de Aparatos Eléctricos y Electrónicos (Waste Electrical and Electronic Equipment directive, WEEE) para el reciclaje de equipo electrónico. El programa le permite devolver un producto de nCipher obsoleto o sobrante, que luego es desechado de forma segura para el medio ambiente. Por más información o para organizar el desecho seguro de su producto, envíe un correo electrónico a nCipher Support.

4 Before installing the module

Figure 1. nShield Solo and nShield Solo XC back panel and jumper switches



nShield Solo



nShield Solo XC

Label	Description
A	Status LED
B	Recessed clear button
C	Physical mode switch

Label	Description
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.

ℹ The configuration of connectors varies between modules and might not be as in *Figure 1. nShield Solo and nShield Solo XC back panel and jumper switches* on page 27.

4.1 Module pre-installation steps

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

- Check the epoxy resin security coating or metal lid of the module 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.
- Check that the two jumper switches are in the required positions (see *Figure 1. nShield Solo and nShield Solo XC back panel and jumper switches* on page 27)
- 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**) (see *Figure 1. nShield Solo and nShield Solo XC back panel and jumper switches* on page 27).

ℹ The default factory setting of the jumper DIP switch **E** is **Off**. This enables remote MOI switching.

ℹ 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.

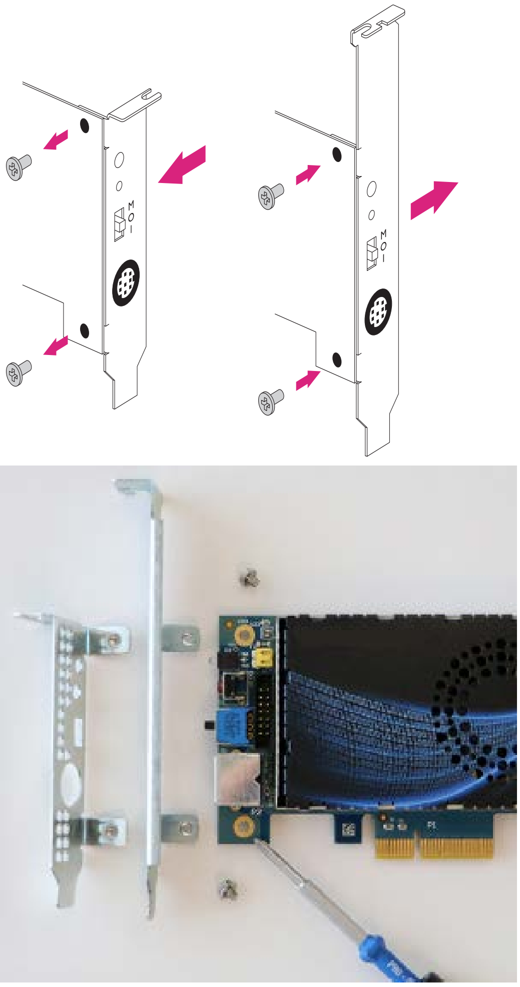
4.2 Fitting a module bracket

Before installing an nShield Solo in a low height card slot, you must replace the standard full height bracket with the low profile bracket supplied with the module.

Before installing an nShield Solo XC in a PCI-Express card slot, you may have to replace the bracket depending on the height of the slot. Both full height and low profile brackets are supplied with the module.

Do not touch the nShield Solo or nShield Solo XC connector pins, or the exposed area of the module without taking ESD precautions.

Figure 2. Removing the low profile bracket (left) and fitting the full height bracket (right)



To fit the full height bracket to the module:

1. Remove the two screws from the solder side of the module.
2. Remove the low profile bracket.
3. Fit the full height 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.

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

4.3 Replace Solo XC Fan

How to replace the Solo XC fan assembly.

Required Tools
Phillips screwdriver #0
Phillips screwdriver #2
Small needle nose pliers
Required Part
Orderable part number SOLOXC-REP-FAN (Replacement fan assembly).

To remove and replace the Solo XC 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 (see *Figure 3. Top cover* on page 30).
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 (see *Figure 4. Removal of fan power cable from P3 connector* on page 31).
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 (see *Figure 5. Power cable grommet identified in the EMI slot* on page 31).
11. Replace the top EMI cover.
12. Re-install the Solo XC into the PCIe slot.

Figure 3. Top cover

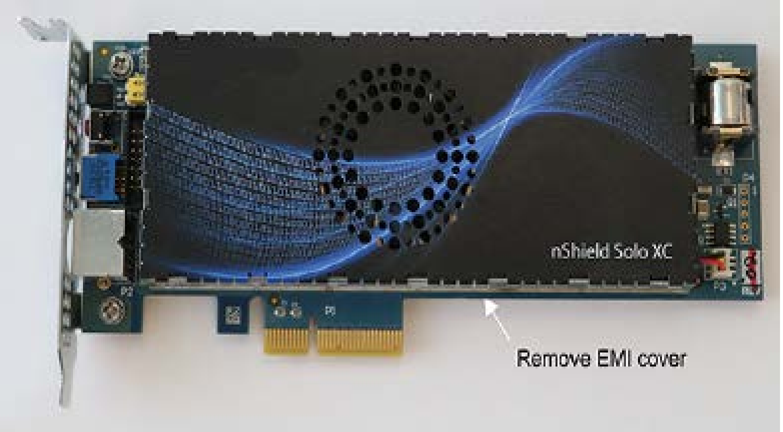


Figure 4. Removal of fan power cable from P3 connector

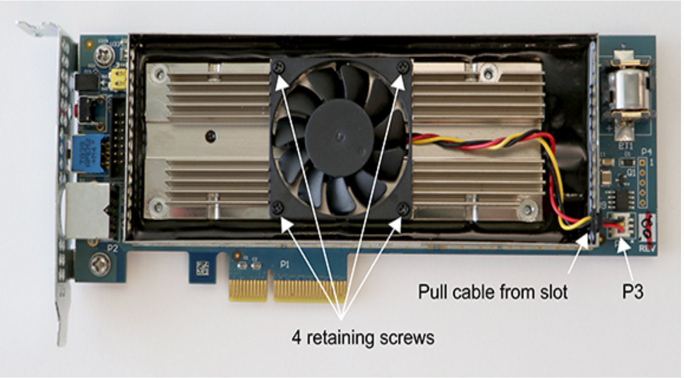
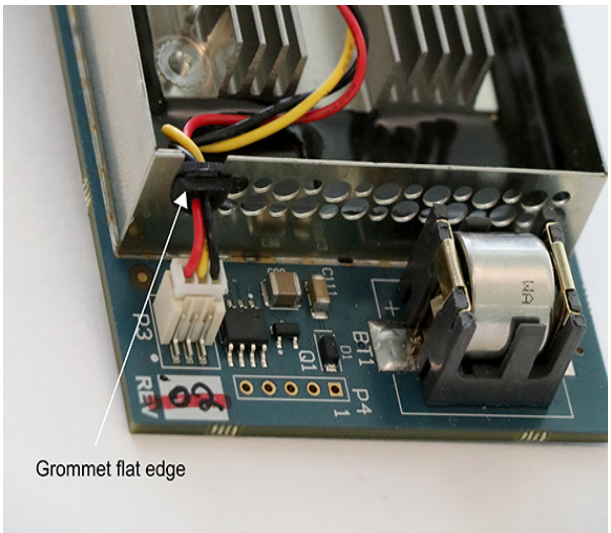


Figure 5. Power cable grommet identified in the EMI slot



4.4 Replace Solo XC Battery

How to replace the Solo XC battery.

Please follow battery disposal guidelines in the installation manual.

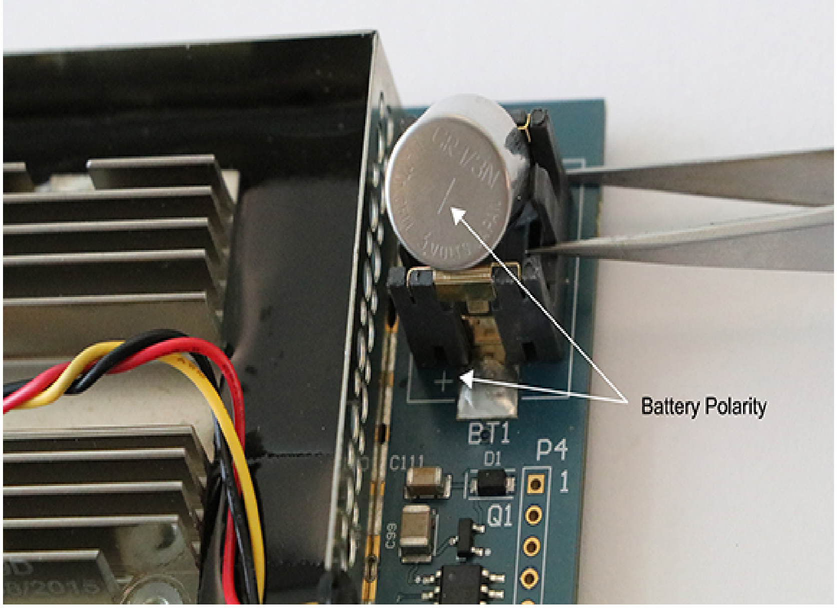
Required Tools
Phillips screwdriver #2
Small tweezers

Required Part
Orderable part number SOLOXC-REP-BATT (Replacement battery)

To remove and replace the Solo XC battery:

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. Using the tweezers, gently remove the battery from the BT1 connector (See *Figure 6. Tweezers removing the battery from the BT1 connector* on page 32).
4. Observing the polarity, install the replacement battery in the BT1 connector.
5. Re-install the Solo XC into the PCIe slot.

Figure 6. Tweezers removing the battery from the BT1 connector



5 Installing the module

To install the module:

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

   The nShield Solo must be fitted to a PCIex1 slot and the nShield Solo XC must be fitted to a PCIEx4 slot.

   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.

   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.

3. 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
4. Use the bracket screw or fixing clip to secure the module to the computer chassis.
5. Check that the two jumper switches on the module are still in required positions (see *Figure 1. nShield Solo and nShield Solo XC back panel and jumper switches* on page 27).
6. Check that the Mode switch is still in the center **O** (operational) position.
7. 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 nShield Solo and nShield Solo XC.

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 nShield Solo or nShield Solo XC. See *Installing the module* on page 33 for more information.
- Uninstall any older versions of Security World Software. See *Uninstalling existing software* on page 54.
- 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 environments

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 Security World Software in a Windows environment* on page 39 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 Unix Environments

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 nCipher Security World Software:

- Java6 (or Java 1.6x)
- Java7 (or Java 1.7x)
- Java8 (or Java 1.8x).

We recommed 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 nCipher 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 nCipher software, please contact nCipher Support.

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 are:

Operating System	Download site
AIX	http://www.ibm.com/developerworks/systems/library/es-JavaOnAix_install.html
HPUX	https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJAVAHOME
various	http://www.oracle.com/technetwork/java/index.html
various	http://www.oracle.com/technetwork/java/all-142825.html

ℹ You must have Java installed to use KeySafe.

6.1.3.2 Identify software components to be installed

nCipher 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.

In Windows environments, you *must* install the **Hardware Support bundle**. If the **Hardware Support bundle** is not installed, your module cannot function.

In Windows environments, the **Windows device drivers** component is installed as part of the **Hardware Support bundle**. In Unix environments, the **Kernel device drivers** component is installed.

In Unix environments, you *must* install the `nfdrv` component.

nCipher recommends that you always install the **Core Tools bundle**. This 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 *Planning to use the Remote Administration Service* on page 36 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 *Components on Security World Software installation media (Windows and Unix)* on page 59 for more about optional components.

6.1.4 Planning to use the Remote Administration Service

The Remote Administration Service should be installed on the host machine of your HSMs and this machine must be accessible to Remote Administration Clients.

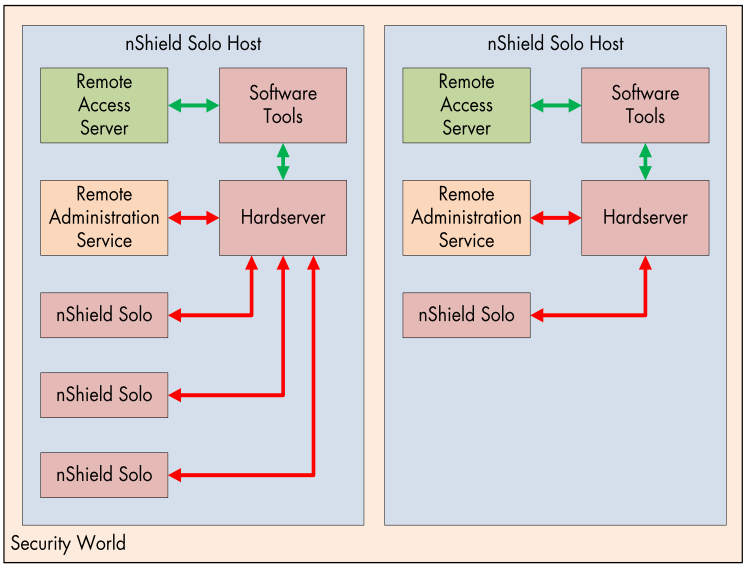
The remote access solution that your organization normally uses, such as SSH or a remote desktop application is also required (illustrated by *Remote Access Server* in *Figure 7. Deploying the Remote Administration Service with an nShield Solo or nShield Solo XC* on page 37).

A secure private communications channel, such as VPN, should always be used for the connection between the Remote Administration Client and the Remote Administration Service if they are on separate computers.

To be able to use an nShield Solo or nShield Solo XC with Remote Administration, you need to make sure that the appropriate firmware (2.61.2 or later) and a KLF2 warrant are installed. See the *User Guide* for more information.

6.1.4.1 The Remote Administration Service with an nShield Solo or nShield Solo XC

Figure 7. Deploying the Remote Administration Service with an nShield Solo or nShield Solo XC



To use Remote Administration with an nShield Solo or nShield Solo XC, the Remote Administration Service must be installed on the host where the hardserver, nShield Solo or nShield Solo XC reside. If you have multiple nShield Solo/nShield Solo XC hosts in a Security World, the Remote Administration Service must be installed on each one.

A privileged connection is required to carry out privileged operations, such as, for example, changing the mode of the nShield Solo or nShield Solo XC.

nShield Remote Administration Cards cannot be used until their serial numbers have been added to the Authorized Card List. See the *User Guide* for further details.

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, eg: • 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 Solo or nShield Solo XC 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

To install the Security World Software in Unix environments, follow the steps that correspond to your Solaris, AIX, HP-UX, or Linux platform.

See the User Guide for more about configuring silent installations and uninstallations under Windows.

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

7.2 Installing Security World Software in a Windows environment

Do the following:

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.exe`** manually if the installer does not run automatically.
3. Follow the onscreen instructions. Accept the license terms.

4. Select all the components required for installation, and then click **Next**. See *Components on Security World Software installation media (Windows and Unix)* on page 59 for more about the component bundles and the additional software supplied on your installation media.

   The selected components are installed in the default directory. The installer creates links to the following nShield Cryptographic Service Provider (CSP) setup wizards under **Start** > **All Programs** > **nCipher**:

   - **nCipher CSP install wizard**, which sets up CSPs for 32-bit applications
   - **nCipher 64bit CSP install wizard**, which sets up CSPs for 64-bit applications

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

5. The installer advises you that the SNMP agent does not run by default. Click **Next** to continue.
6. The installer advises you if you have an existing PKCS #11 installation. Click **Next** to continue.
7. The Security Assurance Mechanism (SAM) for the PKCS #11 library is selected by default. Select **No** if you want to disable the SAM. Click **Next** to continue. See the User Guide for more about the SAM and the available configuration options.
8. Click **Finish** to complete the installation.
9. Update your system environment `PATH` by inserting the sub-path `%NFAST_HOME%\bin`.

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**.

7.3 Installing Security World Software in a Unix Linux environment

7.3.1 Installing on Solaris

To install the Security World Software for Solaris:

1. Log in as a user with root privileges.
2. Place the installation media in the optical disc drive, and mount the drive.
3. To install the Security World Software server, run the command:

   ```
   /usr/sbin/pkgadd -d /cdrom/disc-name/solaris/ver/type/nfast/nfast.pkg
   ```

   In this example, `disc-name` is the mount point of the installation media, `ver` is the version of Solaris (for example, use **11** for Solaris version 11) and `type` is **amd64** for Solaris x86 and **sparc** for Solaris Sparc.

4. From the list of packages available for installation, select all required packages, press `Enter` and follow the on-screen instructions.
5. Run the install script by using the following command:

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

   After the software is installed, you are returned to the shell prompt.

6. 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
     ```

7.3.2 Installing on AIX

To install the Security World Software for AIX:

1. Log in as a user with root privileges.
2. Place the installation media in the optical disc drive, and mount the drive.

3. Start the software management tool by running the command:

   ```
   smit install_latest
   ```

4. Select **List** to display the input device or directory for the software, and select the location that contains the installation image.
5. For **SOFTWARE to install**, select **List**, and then select all required file sets See *Components on Security World Software installation media (Windows and Unix)* on page 59 for more about the component bundles and the additional software supplied on your installation media.
6. Press `Enter` to confirm the file set selection.

   When additional installation options are displayed, leave the default settings enabled. Press `Enter` to confirm these settings, and then press `Enter` again to begin the installation.

7. After software installation is complete, run the install script with the following command:

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

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
     ```

7.3.3 Installing on HP-UX

To install the Security World Software for HP-UX:

1. Log in as a user with root privileges.
2. Place the installation media in the optical disc drive, and mount the drive, using the **`-o cdcase`** option.

3. Open a terminal window, and start the software management tool by running a command of the form:

   ```
   swinstall -s disc-name/hpux/ver/nfast/nfast.dep
   ```

   In this example, `disc-name` is the mount point of the installation media and `ver` is the version of HP-UX (for example, use **11_31** for HP-UX version 11.31).

4. Select all the required software bundles and components for installation. See *Components on Security World Software installation media (Windows and Unix)* on page 59 for more about the component bundles and the additional software supplied on your installation media.
5. Select **Install** from the **Actions** menu.
6. When the installation analysis is complete, click **OK**. If the installer reports any errors, click **Logfile** to display them.
7. Click **Yes** to confirm you want to install.
8. The installer now installs the selected products. When it is complete, click the **Done** button.
9. Log in as **`root`**.
10. Run the install script by using the following command:

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

11. 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
      ```

7.3.4 Installing on Linux

To install the Security World Software for Linux:

1. Log in as a user with root privileges.
2. Place the installation media in the optical disc drive, and mount the drive.
3. Open a terminal window, and change to the root directory.

4. Extract the required `.tar` files to install all the software bundles by running commands of the form:

   ```
   tar xf disc-name/linux/ver/nfast/bundle/file.tar
   ```

   In this command, *ver* is the version of the operating system (for example, **`libc6_11`**), *bundle* is the directory name of a given bundle (for example, **`hwsp`** or **`ctls`**), and *file*`.tar` is the name of a `.tar` file within a bundle directory.

   ℹ Some directories contain more than one `.tar` file.

   See *Components on Security World Software installation media (Windows and Unix)* on page 59 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. nCipher supplies the source to the nCipher PCI kernel driver (**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:

   1. Change directory to the nCipher PCI driver directory by running the command:

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

   2. Configure the source by running the command:

      ```
      # ./configure
      ```

   3. 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 32 bit Windows
- **`C:\Program Files (x86)\nCipher\nfast`** for 64 bit Windows
- **`/opt/nfast`** for Unix-based systems

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

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
```

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* on page 33 for more information. Otherwise, if your system enters Sleep mode, the nShield Solo module may not be found when running **enquiry**. If this happens, 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 prevent 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 *nShield Solo and nShield Solo XC back panel and jumper switches* on page 27).

> 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 prevent 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) in Unix-based Operating Systems.

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 *nSolo 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 operation when the module is powered down. The RTC will not require resetting after the module has been shut down for extended periods. The battery is not rechargeable.

ℹ After upgrading the firmware to an nShield Solo XC board, reboot the host.

9 Status indicators

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 nSheild Solo module is accepting commands. The more frequently the Status LED blinks off, the greater the load on the module. The Status LED will maintain the same operational blink pattern regardless of 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. For more information, see the User Guide.
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 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.

ℹ Use the Mode switch to move between Maintenance, Operational, and Initialization modes. See *Mode switch and jumper switches* on page 50 for more information.

Appendix A Uninstalling existing software

nCipher 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, in Unix environments, a manual installation using `.tar` files *does* overwrite existing data and directories.

ℹ Before you uninstall the Security World Software, nCipher strongly recommends that you make a secure backup of any key data and any existing Security World. See the User Guide for more information.

ℹ 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.

ℹ 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.

ℹ 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 in Unix environments.

nCipher 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.

A.1 Uninstalling Windows software

To uninstall Security World Software in a Windows environment:

1. Open the **Control Panel** and click **Programs and Features**.
2. Select the Security World Software, click **Uninstall**, and follow the on-screen instructions.

A.2 Uninstalling Unix software

A.2.1 Uninstalling on Solaris

To uninstall the Security World Software from Solaris:

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. Remove the software package by running the command:

   ```
   /usr/sbin/pkgrm
   ```

   The command displays the list of components that were installed.

5. Select all the nShield packages (prefixed with the letters **`NC`**), then press `Enter`.
6. Follow the onscreen instructions, confirming the uninstallation of packages as prompted.
7. If you are not planning to re-install the product, delete the configuration file **`/etc/nfast.conf`** if it exists.

ℹ Do not delete the configuration file if you are planning to re-install the product.

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

A.2.2 Uninstalling on AIX

To uninstall the Security World Software from AIX:

1. Log in as a user with root privileges.
2. To remove drivers, install fragments, and scripts and to stop services, run the command:

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

3. Start the software management tool by running the command:

   ```
   smit install_remove
   ```

4. For **SOFTWARE name**, select **List** to list all available file sets, and then select all those prefixed with **ncipher**.
5. Press `Enter` to confirm the selected file sets for uninstallation.

   The **Remove Installed Software** panel is displayed.

6. Ensure that the **PREVIEW Only** option is set to **No** (or the removal operation does not occur), and press `Enter`.
7. When prompted to confirm that you are sure about the removal, press `Enter` again to start the uninstall process.
8. If you are not planning to re-install the product, delete the configuration file **`/etc/nfast.conf`** if it exists.

ℹ Do not delete the configuration file if you are planning to re-install the product.

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

A.2.3 Uninstalling on HP-UX

To uninstall the Security World Software from HP-UX:

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. Remove the software packages by running the command:

```
/usr/sbin/swremove
```

   The command displays the list of components that were installed.

5. Select all the nCipher packages.
6. Select **Remove** from the **Actions** menu.
7. When the analysis is complete, if there are no errors, click **OK**. If the installer reports any errors, click **Logfile** to display them.
8. When the uninstaller asks you to confirm that you want to remove this product, click **Yes**.
9. When the uninstallation is complete, click **Done**.
10. If you are not planning to re-install the product, delete the configuration file **`/etc/nfast.conf`** if it exists.

ℹ Do not delete the configuration file if you are planning to re-install the product.

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

A.2.4 Uninstalling on Linux

To uninstall the Security World Software from Linux:

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
```

⚠ Deleting all the files and subdirectories in **`/opt/nfast`** also deletes the **`/opt/nfast/kmdata`** directory. To be able to restore an existingSecurity 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

5. If you are not planning to re-install the product, delete the configuration file **`/etc/nfast.conf`** if it exists.

ℹ 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.

Appendix B Components on Security World Software installation media (Windows and Unix

This appendix lists the contents of the component bundles and the additional software supplied on your Security World Software installation media. For information on installing the supplied software, see *Installing the software* on page 39.

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

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

B.1 Security World for nShield User installation media

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

B.1.1 Component bundles

Unix Package	Description (Windows and Unix)	Contents of bundle
`hwsp`	**`Hardware Support`** (mandatory)	See *Hardware support*
`ctls`	**`Core Tools`** (recommended)	See *Core tools*
`javasp`	**`Java Support`** (including KeySafe)	See *Java Support (including KeySafe)*
`nhfw`	**`nShield Connect firmware files`**	See *nShield Connect firmware files*
`dsserv`	**`Remote Administration Service`** (optional)	See *Remote Administration Service*
`ratls`	**`Remote Administration Client`** (optional) - Windows and Linux only	See *Remote Administration Client*

B.1.2 Individual components

Unix Package	Description (Windows and Unix)
	`nCipher CAPI-NG providers and tools` - Windows only
`hwcrhk`	`Crypto Hardware Interface (CHIL) plugin`
`jcecsp`	`nCipherKM JCA/JCE provider classes`
	`CSP Console utilities` - Windows only
	`CryptoAPI CSP GUI and console installers` - Windows only
`ncsnmp`	`Net-SNMP monitoring agent, utilities with nCipher MIB functionality`
`pkcs11`	`nCipher pkcs11 library`

B.2 CipherTools installation media

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

B.2.1 Component bundles

Unix Package	Description (Windows and Unix)	Contents of bundle
`hwsp`	`Hardware Support` (mandatory)	See *Hardware support*
`ctls`	`Core Tools` (recommended)	See *Core tools*
`javasp`	`Java Support` (including KeySafe)	See *Java Support (including KeySafe)*
`ctd`	`CipherTools Developer`	See *CipherTools Developer*
`jd`	`Java Developer`	See *Java Developer*
`nhfw`	`nShield Connect firmware files`	See *nShield Connect firmware files*
`dsserv`	`Remote Administration Service` (optional)	See *Remote Administration Service*
`ratls`	`Remote Administration Client` (optional) - Windows and Linux only	See *Remote Administration Client*

B.2.2 Individual components

Unix Package	Description (Windows and Unix)
	`nCipher CAPI-NG providers and tools` - Windows only
`devref`	`nCore API Documentation`
`hwcrhk`	`Crypto Hardware Interface (CHIL) plugin`
`jcecsp`	`nCipherKM JCA/JCE provider classes`
	`CSP Console utilities` - Windows only
	`CryptoAPI CSP GUI and console installers` - Windows only
`ncsnmp`	`Net-SNMP monitoring agent, utilities with nCipher MIB functionality`
`pkcs11`	`nCipher pkcs11 library`
`sslyp`	`Open SSL source code patch file`

B.3 CodeSafe installation media

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

B.3.1 Component bundles

Unix Package	Description (Windows and Unix)	Contents of bundle
`hwsp`	`Hardware Support` (mandatory)	See *Hardware support*
`ctls`	`Core Tools` (recommended)	See *Core tools*
`javasp`	`Java Support` (including KeySafe)	See *Java Support (including KeySafe)*
`csd`	`CodeSafe Developer`	See *CipherTools Developer*
`jd`	`Java Developer`	See *Java Developer*
`nhfw`	`nShield Connect firmware files`	See *nShield Connect firmware files*
`dsserv`	`Remote Administration Service` (optional)	See *Remote Administration Service*
`ratls`	`Remote Administration Client` (optional) - Windows and Linux only	See *Remote Administration Client*

B.3.2 Individual components

Unix Package	Description (Windows and Unix)
	nCipher CAPI-NG providers and tools - Windows only
csdref	nCore CodeSafe API Documentation
devref	nCore API Documentation
gccsrc	Prebuilt arm-gcc for Codesafe/C
gccsrc	Prebuilt powerpcm-gcc for Codesafe/C
hwcrhk	Crypto Hardware Interface (CHIL) plugin
jcecsp	nCipherKM JCA/JCE provider classes
	CSP Console utilities - Windows only
	CryptoAPI CSP GUI and console installers - Windows only
ncsnmp	Net-SNMP monitoring agent, utilities with nCipher MIB functionality
pkcs11	nCipher pkcs11 library

B.4 Common component bundles

nCipher supply component bundles containing many of the necessary components for your installation. Certain standard component bundles are offered for installation on all standard Security World Software installation media, while additional component bundles are found on CipherTools and CodeSafe installation media.

B.4.1 Common component bundles

You are always offered the following standard component bundles on all standard Security World Software installation media:

- Hardware Support
- Core Tools
- Java Support
- nShield Connect firmware files
- Remote Administration Service
- Remote Administration Client.

B.4.1.1 Hardware support

The **Hardware Support** (mandatory) bundle contains the hardserver and kernel device drivers:

Unix Package	Description (Windows and Unix)
	`Windows device drivers` - Windows only
`nfserv`	`Hardserver process executables and scripts`
`sdrv`	`nFast driver signatures`
`cfgall`	`Hardserver config file support`
`nflog`	`Logging library support`

B.4.1.2 Core tools

The **Core Tools** (recommended) bundle contains all the Security World Software command-line utilities, including `generatekey`, low level utilities, and test programs:

Unix Package	Description (WIndows and Unix)
`convrt`	`Command line key conversions`
`nftcl`	`Command line key management (Tcl)`
`nftcl`	`Command line key generation and import`
`nfuser`	`Low level utilities and test programs`
`nfuser`	`Command line remote server management`
`opensl`	`nftcl certificate generation utility`
`sworld`	`Command line key management (C)`
`tclsrc`	`Tcl run time`
`tclstf`	`Small Tcl utilities`
`nftcl`	`Command line key generation and import`
`tct2`	`Trusted Code Tool 2 command-line utility`
`pysrc`	`Python source for developers`
`nfpy`	

nCipher recommend that you always install the **Core Tools bundle**.

The Core Tools bundle includes the `Tcl run time`'s tools for creating the Security World, `KeySafe`, and `new-world`. This does not affect any other installation of Tcl on your computer.

B.4.1.3 Java Support (including KeySafe)

The **Java Support (including KeySafe)** bundle contains Java applications:

Unix Package	Description (Windows and Unix)
`jutils`	`Java utilities`
`jutils`	`JNI shared library for jutils.jar`
`kmjava`	`Java Key Management classes`
`ksafe`	`KeySafe 2`
`nfjava`	`nFast Java generic stub classes`
`nftcl`	`Java Key Management Support`

B.4.1.4 Remote Administration Service

The Remote Administration Service bundle contains the Remote Administration Service installation and configuration. When installed, the Remote Administration Service starts automatically.

B.4.1.5 Remote Administration Client

Graphical User Interface and command line versions of the Remote Administration Client.

B.4.1.6 nShield Connect firmware files

Firmware image files for the nShield Connect. Typically a firmware image file is included that contains the latest FIPS Approved module firmware, as well as the firmware image file for the particular nShield release. In some cases these may be one and the same thing.

B.4.2 Additional component bundles

nCipher supply the following additional component bundles on CipherTools installation media:

- CipherTools Developer
- Java Developer.

nCipher supply the following additional component bundles on CodeSafe installation media:

- Code safe
- Java developer.

B.4.2.1 CipherTools Developer

The **CipherTools Developer** bundle contains components supplied with the CipherTools Developer Kit:

Unix Package	Description (Windows and Unix)
emvspj	JNI library for payShield Java
emvspp	payShield developer library
hwcrhk	Crypto Hardware Interface (CHIL) dev kit
nflibs	nCipher libraries and headers, and example C source for utility functions
nfuser	nCore & KM tools and example source
pkcs11	nFast PKCS#11 developer’s library
sworld	Key Management C library developers kit
tclsrc	Tcl run time - Headers and Libraries
cutils	C utilities library
nflog	Logging library
hilibs	GS libs & headers
pysrc	Python source for developers
nfpy	nFPython header files

B.4.2.2 CodeSafe Developer

The **CodeSafe Developer** bundle contains components supplied with the CodeSafe Developer Kit:

Unix Package	Description (Windows and Unix)
csee	Codesafe-C moduleside example code
csee	Codesafe-C hostside example code
module	Firmware test scripts
nflibs	Generic stub libraries and headers, and example C source for utility functions
nfuser	nCore & KM tools and example source
sworld	Key Management C library developers kit
tclsrc	Tcl run time - Headers and Libraries
cutils	C utilities library
nflog	Logging library
hilibs	GS libs & headers
jhsee	Java hostside developer's kit
jhsee	Java hostside SEE examples
ssllib	Codesafe-SSL hostside code
ssllib	Codesafe-SSL moduleside code
pysrc	Python source for developers
nfpy	nFPython header files
nfpy	Libs and headers for codesafe/python

B.4.2.3 Java Developer

The **Java Developer** bundle contains components to support development of Java applications:

Unix Package	Description (Windows and Unix)
`jcecsp`	`Java Key Management developer`
`jutils`	`Java utilities source and javadocs`
`kmjava`	`Java Key Management developer`
`nfjava`	`Java Generic Stub examples & javadoc`

B.5 Components required for particular functionality

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

If you are planning to use Security World Software with an nShield Edge, ensure that the optional **Edge Monitor Controller** feature is selected during installation.

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

If you have CipherTools installation media, nCipher recommend that you install the **CipherTools Developer** bundle.

If you have CodeSafe installation media, nCipher recommend that you install the **CodeSafe Developer** bundle.

If you have CodeSafe installation media and you are developing in C:

- If your module has a part code of the form nC4*nn*2 or Bn1*nnn*, install the **Prebuilt arm-gcc for Codesafe/C** component.
- If your module has a part code of the form nC4*nn*3, Bn2*nnn*, BN2*nnn(-E)*, or NH2*nnn*, install the **Prebuilt powerpc-gcc for Codesafe/C** component.

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

If you have CipherTools installation media or CodeSafe installation media and 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 `nfdrvk` component if you are using a nCipher PCI card.

B.5.1 KeySafe

To use KeySafe, install the **Core Tools** and the **Java Support (including KeySafe)** bundles.

B.5.2 Microsoft CAPI CSP

If you require the Microsoft CAPI CSP, you must install the CSP components:

- **CSP console utilities**
- **CryptoAPI CSP GUI and console installers**

B.5.3 Microsoft Cryptography API: Next Generation (CNG)

If you require the Microsoft CNG, you must install the CNG component:

nCipher CAPI-NG providers and tools

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, Red Hat Certificate System install the **`nCipher 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 the nCipher web site: https://www.ncipher.com.

B.6 Cryptographic Hardware Interface Library applications

If you want to use the module with the Cryptographic Hardware Interface Library (CHIL) applications, install the **Crypto Hardware Interface (CHIL) plugin** component and, if required, the **OpenSSL source code patch file** component.

Security World Software supports OpenSSL 1.0.1g and later.

B.7 nCipherKM JCA/JCE cryptographic service provider

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

- The **Java Support (including KeySafe)** bundle
- The **nCipherKM JCA/JCE provider classes** component

An additional JCE provider **nCipherRSAPrivateEncrypt** is supplied that is required for RSA encryption with a private key. Install this provider and ensure that the file **rsaprivenc.jar** is in your **CLASSPATH**.

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

B.8 SNMP monitoring agent

If you want to use the SNMP monitoring agent to monitor your modules, install the **SNMP monitoring agent** component. During the first installation process of the SNMP agent, the agent displays the following message:

```
If this is a first time install, the nCipher 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.

Appendix C Virtualization Remote Server

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

- **Microsoft Hyper-V**, a role in Windows Server 2012 and Windows Server 2016 used to create and manage a virtualized server computing environment

  Hyper-V virtualizes hardware to provide an environment where multiple operating systems can run at the same time on one physical computer. Each virtual machine is an isolated, virtualized computer system that can run its own operating system.

- **VMware vSphere hypervisor, ESXi** – no underlying operating system

  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.

PCI applies to VMWare.

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.

C.1 Virtualization and Hyper-V

The host hardserver is configured to run on the Parent/Dom0 operating system. The Parent/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.

C.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.

C.3 ESXi environment

After installing VMware ESXI 5.5, the VM guest can be remotely managed and the PCI passthrough of the Solo module configured using vSphere client 5.5. PCI passthrough allows a VM guest direct access to the nShield Solo XC.

C.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 5.1 Documentation Center, see https://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.solutions.doc/GUID-3B52FFD2-2A7E-45E7-BE2A-A35413220221.html.
3. Install the vSphere Web Client using the instructions provided in the VMware vSphere 5.1 Documentation Center,see https://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.solutions.doc/GUID-3B52FFD2-2A7E-45E7-BE2A-A35413220221.html.

C.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**.

The ESXi 5.5 will now be successfully installed and the Solo PCIe module has been configured for passthrough.

C.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 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 guest 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 the **Typical Configuration** radio button 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) (radio button) 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 requirement for IP communication between the two.

    a. Datastore: **<datastore1>**
    b. Available space (GB): **<357.3>**
    c. Virtual disk size: **50 GB**
    d. Select the radio button for **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**.

C.4 XenServer environments

Install the XenServer, follow the instructions in the Citrix XenServer Quick Start Guide. see https://www.citrix.com.

C.4.1 Configure the XenCenter 6.5 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 (i.e., 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
    ```

ℹ 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>
```

ℹ When the installation of XenCenter has completed you can access `[https://( XENSERVERIP)]` to acquire the corresponding XenCenter Client Remote management interface.

C.4.2 Create a XenServer guest instance and hardserver configuration

ℹ 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 **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**.

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

ℹ 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.

C.5 Hyper-V environment (Windows Server 2012)

C.5.1 Install Hyper-V on the server

To install the Hyper-V, see https://technet.microsoft.com/en-us/library/hh846766.aspx.

C.5.2 Add the Hyper-V role to the server

To add the Hyper-V role in Windows server:

1. Logon as Administrator.
2. Open **Server Manager**.
3. Select **Manage**.
4. Select **Add Roles and Features**.
5. Select **Next**.
6. Select the **Role-based or feature-based installation** button.
7. Select **Next**.
8. Select the **Select a server from the server pool** button.
9. Select a server that has Windows 2012 R2 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 2012 R2 instance.

C.5.3 Configure Hyper-V

To configure Hyper-V:

1. Open the **Server Manager**.
2. Select **Tools**.

    Hyper-V Manager is the GUI application that enables you to create virtual machine guest instances.

3. Select **Hyper-V Manager**.

4. Select **Virtual Switch Manager** from the **Actions** page.

   Using the Virtual Switch Manager you can create External, Internal, and Private switches. The differences between the virtual switch types:

   - External: the VM guest can communicate to the open internet, host Parent partition, and other VM guests
   - Internal: the VM guest can communicate amongst other VM guests and the host Parent partition
   - Private: VM guests can only communicate amongst each other.
5. Select **New virtual network switch**.
6. Select the required switch (**External**, **Internal** or **Private**).
7. Select **Create Virtual Switch**.
8. Select **New Virtual Switch**.
9. Enter a name for the switch.
10. Select the **External network** under **Connection** type.
11. Select **Allow management operating system to share this network adapter**.
12. Select **Apply**.
13. The Network card is now exposed to the external network and the virtual switch is ready for VMs guest configurations.

C.5.4 Create the VM guest instance and hardserver configuration

The steps to create a VM guest instance are the same for all three virtual switch types.

C.5.4.1 Install the CipherTools software:

Install the CipherTools 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 CipherTools software. The CipherTools software will auto install.
2. 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. See *Checking the installation* in the *nShield Solo Installation Guide*.

C.5.4.2 Configure the hardserver to export the module to guest VM usage

To configure the hardserver to export the module to guest VM usage:

These commands can be repeated for any number of guests.

1. Run the command:

```
Root@<userid>-HVM-domU: /opt/nfast/bin# ./rserverperm –add -a <IPv4 of the 1st Guest VM
created in which a guest hardserver is running> --exportslot
```

```
System response: OK permission ID is 2
```

2. Run the command:

```
Root@<userid>-HVM-domU: /opt/nfast/bin# ./rserverperm –add -a <IPv4 of the 1st Guest VM
created in which a guest hardserver is running > --exportmodule
```

```
System response: OK permission ID is 3
```

C.5.4.3 Configure the second guest VM instance

To configure the hardserver to export the module to guest VM instance:

1. Run the command:

```
Root@<userid>-HVM-domU: /opt/nfast/bin# ./rserverperm –add -a <IPv4 of the 2nd Guest VM
in which a guest hardserver is running > --exportslot
```

```
System response: OK permission ID is 2
```

2. Run the command:

```
Root@<userid>-HVM-domU: /opt/nfast/bin# ./rserverperm –add -a <IPv4 of the 2nd Guest VM
in which a guest hardserver is running > --exportmodule
```

C.5.4.4 Configure the hardserver to enroll to the primary guest hardserver via IP address using the virtual switch

Enter the following commands for each guest hardserver:

1. Run the commands:

```
Root@<userid>-HVM-domU: /opt/nfast/bin# ./anonkneti <IP of the 1st Guest VM created>
Root@<userid>-HVM-domU: /opt/nfast/bin# ./nethsmenroll –force <IP of the 1st Guest VM
created>
```

```
System response: Is the above correct
```

2. Enter **Yes** and press enter.

```
System response: OK  configuring hardserver’s nethsm imports
```

C.5.4.5 Confirm the connection to the second guest VM

To confirm the connection with the second guest VM:

1. 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. See *Checking the installation* in the *nShield Solo Installation Guide*.

C.5.4.6 Create secondary WM guests

To create secondary VM guests:

1. Open the Hyper-V Manager within your Windows 2012 R2 server.
2. Logon 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.

   ℹ Use the default location setting.

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

   ℹ For example, Generation 2 is selected. Generation 2 is valid for products such as Windows 8 and beyond and with Windows Server 2012

8. Select **Next**.
9. Select an amount of memory for allocation to this guest VM instance.

10. Select **Next**.

    On the Configure Networking screen, you must select the same virtual switch that was created as guest VM in order to provide the hardserver instance within each guest VM the ability to send requests to the nSheild Solo XC module that is physically connected to the NFAST service installed in the Windows 2012 R2 host hardserver.

11. Select the virtual switch for Connection from the drop down list.
12. Select **Next**.
13. Select the button for **Create a virtual hard disk**.
14. Enter **Name**, **location** and **size**.
15. Select **Next**.
16. 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**
17. Select **Next**.
18. Select **Finish**.

C.6 Hyper-V environment (Windows Server 2016)

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.

C.6.1 Set up

C.6.1.1 Install Hyper-V on the server

To install the Hyper-V, see https://docs.microsoft.com/en-gb/windows-server/virtualization/hyper-v/get-started/Install-the-Hyper-V-role-on-Windows-Server.

C.6.1.2 Add the Hyper-V role to the server

To add the Hyper-V role in Windows server:

1. Logon as Administrator.
2. Open **Server Manager**.
3. Select **Manage**.
4. Select **Add Roles and Features**.
5. Select **Next**.
6. Select the **Role-based or feature-based installation** button.
7. Select **Next**.
8. Select the **Select a server from the server pool** button.
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.

C.6.1.3 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
```

C.6.1.4 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
   ```

C.6.1.5 Install the CipherTools software

Install the CipherTools 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 CipherTools software. The CipherTools software will auto install.
2. 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. See *Checking the installation* in the *nShield Solo Intallation Guide*.

C.6.1.6 Create the VM guest instance on the server

1. Open the Hyper-V Manager within your Windows 2016 server.
2. Logon 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 button next to 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 the button for **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**.

C.6.1.7 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
```

ℹ To find the $locationPath run the command:

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

ℹ 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* on page 85.

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

C.6.2 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}
```

C.6.3 Undo Passthrough

1. Mount a single device. Run the command:

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

ℹ 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
```

ℹ To find the $locationPath run the command:

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