



**ENTRUST**

nShield Security World

# **nShield Connect v12.40 Installation Guide**

04 March 2024

---

# Contents

<b>Chapter 1: Introduction</b> .....	<b>8</b>
About this guide .....	8
Model numbers .....	9
Power and safety requirements .....	9
Additional documentation .....	9
Terminology .....	9
Typographical conventions .....	10
Avertissements relatifs à la sécurité pour le nShield Connect .....	10
nShield Connect- Sicherheitswarnungen .....	11
Handling an nShield Connect .....	11
Weight and Dimensions .....	12
Environmental requirements .....	12
Temperature and humidity recommendations .....	12
Cooling requirements .....	12
Physical location considerations .....	13
<b>Chapter 2: Regulatory notices</b> .....	<b>14</b>
FCC class A notice .....	14
Canadian certification - CAN ICES-3 (A)/NMB- 3(A) .....	14
Recycling and disposal information .....	14
<b>Avis juridiques</b> .....	<b>15</b>
Classe A de la FCC .....	15
Certification canadienne - CAN ICES-3 (A)/NMB- 3(A) .....	15
Information concernant le recyclage et le traitement .....	15
<b>Rechtliche Informationen</b> .....	<b>16</b>
Hinweis FCC-Klasse A .....	16
Kanadische Zertifizierung - CAN ICES-3 (A)/NMB- 3(A) .....	16
Informationen zu Recycling und Entsorgung .....	16

<b>Notificaciones reglamentarias</b> .....	<b>17</b>
Notificación clase A de la FCC .....	17
Certificación de Canadá - CAN ICES-3 (A)/NMB- 3(A) .....	17
Información de desecho y reciclaje .....	17
<b>Chapter 3: Before you install the software</b> .....	<b>18</b>
Preparatory tasks before installing software .....	18
Windows environments .....	18
Unix Environments .....	18
All environments .....	19
Planning to use the Remote Administration Service .....	20
Firewall settings .....	22
<b>Chapter 4: Installing the software</b> .....	<b>23</b>
Installing the Security World Software .....	23
Installing Security World Software in a Windows environment .....	23
Installing Security World Software in a Unix Linux environment .....	24
Installing on Solaris .....	24
Installing on AIX .....	24
Installing on HP-UX .....	25
Installing on Linux .....	26
Checking the installation .....	28
<b>Chapter 5: Before installing an nShield Connect</b> .....	<b>29</b>
Carefully unpack the nShield Connect .....	29
Check that all parts on the packing list are present .....	29
Check the physical security of the nShield Connect .....	29
<b>Chapter 6: Installing an nShield Connect in a rack, cabinet, or shelf</b> .....	<b>30</b>
Connecting Ethernet and power cables .....	31
Connecting the optional USB keyboard .....	32
Configuring an nShield Connect for your keyboard type .....	32
Checking the installation .....	32
<b>Chapter 7: Basic nShield Connect and client configuration</b> .....	<b>33</b>

About nShield Connect and client configuration .....	33
Remote file system (RFS) .....	33
nShield Connect configuration .....	34
Client configuration .....	34
Basic nShield Connect and RFS configuration .....	34
Configuring the Ethernet interfaces - IPv4 and IPv6 .....	34
Configure Ethernet Interface #1 .....	38
Configure Ethernet Interface #2 .....	41
Default gateway .....	41
Set up Routing .....	42
Edit route entry .....	44
Remove route entry .....	46
Enable IPv6 SLAAC .....	46
Configuring the Remote File System (RFS) .....	46
Basic configuration of the client to use the nShield Connect .....	48
Client configuration utilities .....	48
Configuring a client to communicate through an nToken .....	50
Enrolling the client from the command line .....	50
Configure the TCP sockets on the client for Java applications (for example, KeySafe) .....	51
Basic configuration of an nShield Connect to use a client .....	52
Using a Security World .....	54
<b>Chapter 8: Front panel controls .....</b>	<b>55</b>
<b>Chapter 9: Top-level menu .....</b>	<b>56</b>
1 System .....	57
2 HSM .....	58
3 Security World mgmt .....	59
<b>Chapter 10: Troubleshooting .....</b>	<b>60</b>
Checking operational status .....	60
Enquiry utility .....	60
Status LED .....	61

Audible warning .....	62
Orange warning LED .....	62
Checking the physical security of the module .....	62
Display screen .....	62
Power button .....	63
Ethernet LEDs .....	63
Module overheating .....	64
Log messages for the module .....	64
Information .....	64
Notice .....	64
Client .....	64
Serious error .....	65
Serious internal error .....	65
Start-up errors .....	65
Fatal errors .....	65
Utility error messages .....	66
BadTokenData error in nShield modules .....	66
<b>Chapter 11: nShield Connect maintenance .....</b>	<b>67</b>
Flash testing the module .....	67
<b>Chapter 12: Approved accessories .....</b>	<b>68</b>
<b>Appendix A: Uninstalling existing software .....</b>	<b>69</b>
Uninstalling Windows software .....	69
Uninstalling Unix software .....	70
Uninstalling on Solaris .....	70
Uninstalling on AIX .....	71
Uninstalling on HP-UX .....	72
Uninstalling on Linux .....	72
<b>Appendix B: Components on Security World Software installation media (Windows and Unix) .....</b>	<b>74</b>
Security World for nShield User installation media .....	74
Component bundles .....	74

---

Individual components .....	75
CipherTools installation media .....	75
Component bundles .....	75
Individual components .....	76
CodeSafe installation media .....	76
Component bundles .....	76
Individual components .....	77
Common component bundles .....	78
Common component bundles .....	78
Additional component bundles .....	80
Components required for particular functionality .....	83
KeySafe .....	84
Microsoft CAPI CSP .....	84
Microsoft Cryptography API: Next Generation (CNG) .....	84
Cryptographic Hardware Interface Library applications .....	84
nCipherKM/JCA/JCE cryptographic service provider .....	85
SNMP monitoring agent .....	85
<b>Appendix C: Valid IPv6 Addresses .....</b>	<b>86</b>

# Chapter 1: Introduction

The nShield® Connect is a *Hardware Security Module (HSM)* that provides secure cryptographic processing within a tamper-resistant casing. Each nShield Connect is configured to communicate with one or more client computers over an Ethernet network. A client is a computer using the nShield Connect for cryptography. You can also configure clients to use other nShield Connects on the network, as well as locally installed HSMs.

## About this guide

This guide includes:

- Installing the Security World Software. See *Chapter 4: Installing the software on page 23*.
- Physically installing an nShield Connect. See *Chapter 6: Installing an nShield Connect in a rack, cabinet, or shelf on page 30*.
- Configuring an nShield Connect and client. See *Chapter 7: Basic nShield Connect and client configuration on page 33*.
- The nShield Connect front panel controls. See *Chapter 8: Front panel controls on page 55*.
- The top-level menu of an nShield Connect. See *Chapter 9: Top-level menu on page 56*.
- Troubleshooting information. See *Chapter 10: Troubleshooting on page 60*.
- nShield Connect maintenance. See *Chapter 11: nShield Connect maintenance on page 67*.
- Accessories. See *Chapter 12: Approved accessories on page 68*.
- Instructions to uninstall existing software. See *Appendix A: Uninstalling existing software on page 69*.
- Software components and bundles. See *Appendix B: Components on Security World Software installation media (Windows and Unix) on page 74*.

See the *nShield Connect 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 Connect

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

## Model numbers

The table below shows the different versions of the module.

Model number	Used for
NH2047	nShield Connect 6000
NH2040	nShield Connect 1500
NH2033	nShield Connect 500
NH2068	nShield Connect 6000+
NH2061	nShield Connect 1500+
NH2054	nShield Connect 500+
NH2075-B	nShield Connect XC Base
NH2075-M	nShield Connect XC Mid
NH2075-H	nShield Connect XC High
NH2082	nShield Connect XC SCAP

## Power and safety requirements

The module draws up to 220 watts:

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

**Note:** The module PSUs are compatible with international mains voltage supplies.

## Additional documentation

You can find additional documentation in the **document** directory of the installation media for your product.

For information about enabling additional features (such as client licences), see the User Guide.

We strongly recommend that you read the release notes in the **re1ease** directory of your installation disc before you use the module. These notes contain the latest information about your product.

See the User Guide for a glossary of terms.

## Terminology

The nShield Connect is referred to as the *nShield Connect*, the *hardware security module*, or the *HSM*.

The internal security module of the nShield Connect is referred to as the *internal security module*.

When nCipher hardware security products are referred to in general, the term *hardware security module* or *HSM* is used.



## Typographical conventions

**Note:** 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

## Avertissements relatifs à la sécurité pour le nShield Connect

Avec le nShield Connect, conformez-vous systématiquement aux précautions de sécurité suivantes:



N'effectuez de branchement qu'aux prises d'alimentation reliées à la terre. Le nShield Connect est un matériel de Classe 1 et il doit être relié à la terre.



N'effectuez de branchement qu'à une prise d'alimentation électrique présentant une tension correspondant à celle indiquée sur la plaque signalétique. La plaque signalétique est située en dessous du produit.



Pour déconnecter le nShield Connect, assurez-vous que les cordons secteur IEC ou les prises électriques sont facilement accessibles.



Pour isoler le courant, retirez tous les câbles électriques du nShield Connect (reportez-vous aux instructions affichées à l'arrière de l'unité, au dessus de chaque bloc d'alimentation).



Utilisez systématiquement les câbles électriques fournis avec le nShield Connect.



Le goujon M4 situé sur le panneau arrière du nShield Connect constitue une mise à la terre fonctionnelle destinée à la CEM. Ne branchez pas de conducteurs protecteurs de mise à la terre à ce terminal.



Ne branchez pas les prises RJ45 à un équipement réseau situé à l'extérieur du bâtiment ou à l'équipement de télécommunications.

## nShield Connect- Sicherheitswarnungen

Beachten Sie bei Verwendung des nShield Connect stets folgende Sicherheitsvorkehrungen:



Nur mit geerdeten Anschlussbuchsen verbinden. Das nShield Connect hat die Bauklasse 1 und muss geerdet werden.



Nur mit Steckdosen verbinden, deren elektrische Spannung der Angabe auf dem Leistungsschild entspricht. Das Leistungsschild ist an der Unterseite des Gerätes nahe der Rückseite angebracht.



Stellen Sie sicher, dass die IEC-Buchsen des Kabelsets bzw. die Netzstecker gut zugänglich sind, damit Sie das nShield Connect jederzeit abtrennen können.



Um das Modul von der Stromversorgung abzutrennen, entfernen Sie alle Netzkabel von dem nShield Connect — siehe hierzu Anweisungen auf der Rückseite der Einheit über den einzelnen Stromversorgungseinheiten (PSUs).



Verwenden Sie ausschließlich die dem nShield Connect beiliegenden Netzkabel.



Der M4-Stift auf der Rückseite des nShield Connect ist ein Funktionserdungsterminal zur EMV-Filterung. Verbinden Sie keine Schutzerdungsleiter mit diesem Terminal.



Verbinden Sie RJ45-Stecker nie mit Netzwerkgeräten außerhalb des Gebäudes oder mit Telekommunikationsausrüstung.

## Handling an nShield Connect

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



If you are installing the module in a 19" rack, make sure that you follow the *nShield Connect Slide Rails Instructions* provided with the rails. In particular, be careful of sharp edges.

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

## Weight and Dimensions

Weight: 11.5kg

Dimensions: 43.4mm x 430mm x 690mm

**Note:** The module is compatible with 1U 19" rack systems.

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

## Environmental requirements

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

## Temperature and humidity recommendations

We recommend that your module operates within the following environmental conditions.

Environmental conditions	Operating range		Comments
	Min.	Max.	
Guaranteed operating temperature	10°C	35°C	Guaranteed performance within this temperature range.
Operating temperature	5°C	40°C	-
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.
Altitude	-100m	2000m	Above Mean Sea Level (AMSL)



The nShield Connect is designed to operate in moderate climates only. Never operate the module in dusty, damp, or excessively hot conditions.

Never install, store, or operate the module at locations where it might be subject to dripping or splashing liquids.

## Cooling requirements

Adequate cooling of your 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. You are advised to do this directly after installing the unit in its normal working environment. Monitor the temperature of the unit over its first few days of operation.

In the unlikely event that the internal encryption module overheats, the module shuts down (see [Module overheating on page 64](#)). If the whole nShield Connect overheats, the orange warning LED on the front panel illuminates (see [Orange warning LED on page 62](#)) and a critical error message is shown on the display.



To help ensure adequate cooling, check that the front and the rear vents on the module are not blocked.

## 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.

# Chapter 2: Regulatory notices

## FCC class A notice

This nShield Solo HSM complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This 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.

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

### 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 Security 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 [recycling@ncipher.com](mailto:recycling@ncipher.com).

# Avis juridiques

## 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.

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

### 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 Security 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 [recycling@ncipher.com](mailto:recycling@ncipher.com).

# Rechtliche Informationen

## 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 Wohngebieten kann möglicherweise störende Interferenzen verursachen. In einem solchen Fall muss der Nutzer die Interferenzen auf seine eigenen Kosten abstellen.

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

### Informationen zu Recycling und Entsorgung

Gemäß der WEEE-Richtlinie (Waste Electrical and Electronic Equipment) wird zur Wiederverwertung von elektronischen Geräten ein Rücknahme- und Recyclingprogramm bereitgestellt. Im Rahmen dieses Programms können Sie veraltete oder nicht mehr genutzte nCipher Security 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 [recycling@ncipher.com](mailto:recycling@ncipher.com).

# Notificaciones reglamentarias

## Notificación clase A de la FCC

Este HSM nShield Solo cumple con la parte 15 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.

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

### 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 Security 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 [recycling@ncipher.com](mailto:recycling@ncipher.com).



# Chapter 3: Before you install the software

Before you install the software, you should:

- Install an optional nToken in the client computer, if required see *nToken Installation Guide* for more information about the installation steps.
- Uninstall any older versions of Security World Software. See *Appendix A: Uninstalling existing software* on page 69.
- Complete any other necessary preparatory tasks, as described in *Preparatory tasks before installing software*.

## Preparatory tasks before installing software

Perform any of the necessary preparatory tasks described in this section before installing the Security World Software on the client computer.

### Windows environments

Adjust your computers power saving setting to prevent sleep mode.

### 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/>.

### Unix Environments

#### Install operating environment patches

Make sure that you have installed the latest recommended patches. See the documentation supplied with your operating environment for information.

#### 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.

## All environments

### 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:

- Java5 (or Java 1.5x)
- Java6 (or Java 1.6x)
- Java7 (or Java 1.7x)
- Java8 (or Java 1.8x).

We recommend 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	<a href="http://www.ibm.com/developerworks/systems/library/es-JavaOnAix_install.html">http://www.ibm.com/developerworks/systems/library/es-JavaOnAix_install.html</a>
HPUX	<a href="https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJAVAHOME">https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJAVAHOME</a>
various	<a href="http://www.oracle.com/technetwork/java/index.html">http://www.oracle.com/technetwork/java/index.html</a>
various	<a href="http://www.oracle.com/technetwork/java/all-142825.html">http://www.oracle.com/technetwork/java/all-142825.html</a>

**Note:** You must have Java installed to use KeySafe.

### 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.

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

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

**Note:** 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 20](#) and the *User Guide* for more about the Remote Administration Service.

**Note:** 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 [Appendix B: Components on Security World Software installation media \(Windows and Unix\) on page 74](#) for more about optional components.

## Planning to use the Remote Administration Service

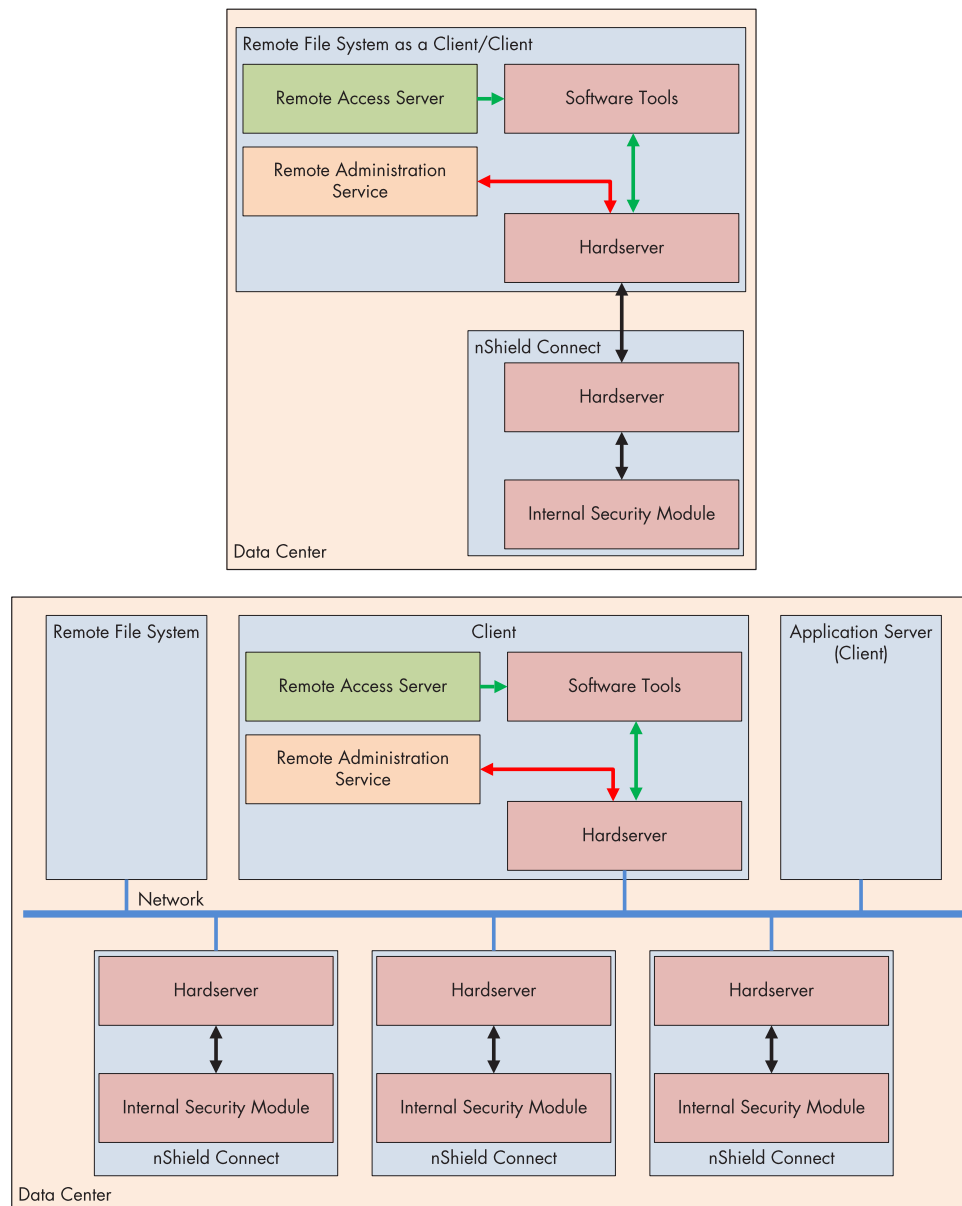
The Remote Administration Service should be installed on a client machine of the HSMs in your Security World that you can make accessible to Remote Administration Clients.

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 1. Deploying the Remote Administration Service with nShield Connects** on page 21 ).

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.

## The Remote Administration Service with nShield Connects

Figure 1. Deploying the Remote Administration Service with nShield Connects



**Note:** The Remote Access Server can be on a different client to the one where the Remote Administration Service is installed.

To use Remote Administration with nShield Connects, the Remote Administration Service must be installed on a client, which may also be the RFS. The client must allow privileged connections.

The Remote Administration Service does not require a dedicated server.

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

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.

## 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
		Incoming impath connections from other hardservers, eg:
Hardserver	9004	<ul style="list-style-type: none"> <li>From a nShield Connect to the Remote File System (RFS)</li> <li>From a non-attended nShield Connect to an attended host machine when using Remote Operator</li> </ul>
Hardserver in nShield Connect	9004	Incoming impath connections from client machines
Remote Administration Service	9005	Incoming connections from Remote Administration Clients

If you are setting up an RFS or exporting a slot for Remote Operator functionality, you need to open port 9004. You may restrict the IP addresses to the addresses 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.

# Chapter 4: Installing the software

This chapter describes how to install the Security World Software on the computer, client, or RFS associated with your nShield HSM.

After you have installed the software, you must complete further Security World creation, configuration and setup tasks before you can use your nShield environment to protect and manage your keys. See the User Guide for more about creating a Security World and the appropriate card sets, and further configuration or setup tasks.

## 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 uninstalls under Windows.

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

## Installing Security World Software in a Windows environment

Do the following:

1. Log in as Administrator or as a user with local administrator rights.
  - Note:** 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.
3. Place the Security World Software installation media in the optical disc drive. Launch **setup.exe** manually if the installer does not run automatically.
4. Follow the onscreen instructions. Accept the license terms.
5. Select all the components required for installation, and then click **Next**. See [Appendix B: Components on Security World Software installation media \(Windows and Unix\)](#) on page 74 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
7. The installer advises you that the SNMP agent does not run by default. Click **Next** to continue.
8. The installer advises you if you have an existing PKCS #11 installation. Click **Next** to continue.
9. 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.

10. Click **Finish** to complete the installation.
11. Update your system environment **PATH** by inserting the sub-path `%NFAST_HOME%\bin`.

## Installing Security World Software in a Unix Linux environment

### 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
```

---

### 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 [Appendix B: Components on Security World Software installation media \(Windows and Unix\)](#) on page 74 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
```

---

## 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.



- 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).

- Select all the required software bundles and components for installation. See [Appendix B: Components on Security World Software installation media \(Windows and Unix\)](#) on page 74 for more about the component bundles and the additional software supplied on your installation media.
- Select **Install** from the **Actions** menu.
- When the installation analysis is complete, click **OK**. If the installer reports any errors, click **Logfile** to display them.
- Click **Yes** to confirm you want to install.
- The installer now installs the selected products. When it is complete, click the **Done** button.
- Log in as **root**.
- Run the install script by using the following command:

---

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

---

- 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
```

---

## Installing on Linux

To install the Security World Software for Linux:

- Log in as a user with root privileges.
- Place the installation media in the optical disc drive, and mount the drive.
- 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 `ct1s`), and *file.tar* is the name of a `.tar` file within a bundle directory.

**Note:** Some directories contain more than one `.tar` file.

See [Appendix B: Components on Security World Software installation media \(Windows and Unix\) on page 74](#) for more about the component bundles and the additional software supplied on your installation media.

5. Run the install script by using the following command:

---

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

---

6. Log in to your normal account.
7. Add `/opt/nfast/bin` to your `PATH` system variable:
  - If you use the Bourne shell, add these lines to your system or personal profile:

---

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

---

- If you use the C shell, add this line to your system or personal profile:

---

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

---

## Checking the installation

To check that the module is installed and configured correctly on the client:

1. Log in as a user and open a command window.
2. Run the command:

---

```
enquiry
```

---

3. The following is an example of the output following a successful **enquiry** command:

---

```
Module ##:
enquiry reply flags none
enquiry reply level Six
serial number #####-####-####
mode operational
version #.#.#
speed index #####
rec. queue ##.##
...
version serial ##
connection status OK
connection info esn = #####-####-####; addr = #####/###.##.##.###/#####; ku hash =
xxxxx, mech = Any; time-limit = 24h; data-limit = 8MB
image version #.#.#####
max exported modules 3
rec. LongJobs queue ##
SEE machine type PowerPCSXF
supported KML types DSAP1024s160 DSAP3072s256
using impath kx grp DHPrime3072
hardware status OK
```

---

If you are configuring a client belonging to an nShield Connect, the response to the **enquiry** command should be populated and the **hardware status** shown as **OK**.

If the **mode** is **operational** the HSM has been installed correctly.

If the **mode** is **initialization**, the HSM has been installed correctly, but you must change the mode to **operational**.

If the output from the **enquiry** command says that the module is not found, first restart your computer, then re-run the **enquiry** command.

# Chapter 5: Before installing an nShield Connect

## Carefully unpack the nShield Connect



Retain all parts of the nShield Connect packaging, including the outer (brown) shipping carton, in case you have to return the HSM. Your warranty or maintenance agreement does not cover returned modules that are damaged due to shipping in non-approved packaging.

## Check that all parts on the packing list are present

The packing list contains a full list of items shipped with the HSM. If any item is missing, contact Support.

**Note:** Any optional parts ordered, for example slide rail components, might not appear on the packing list. If any optional components are missing, contact Support.

## Check the physical security of the nShield Connect

See the *nShield Connect Physical Security Checklist*, provided in the box with an nShield Connect and available in the **document** folder on the installation media.



Breaking the security seal or dismantling the nShield Connect voids your warranty cover, and any existing maintenance and support agreements.

# Chapter 6: Installing an nShield Connect in a rack, cabinet, or shelf

This chapter describes how to install the nShield Connect. For more information about connecting the nShield Connect to the network, and configuring it for connection to one or more clients on the network, see the *nShield Connect User Guide*.



Always handle modules correctly. For more information, see *Handling an nShield Connect on page 11*.

Take due account of the weight and dimensions of the nShield Connect when selecting a location for storage or installation ( see *Handling an nShield Connect on page 11*).

**Note:** You cannot install or configure the nShield Connect remotely.

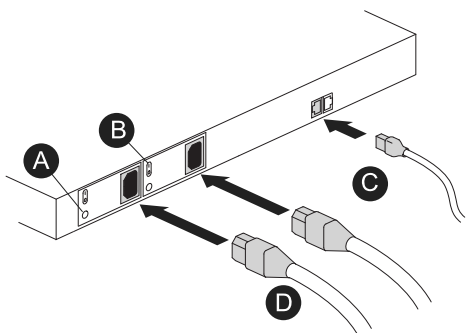
To install the nShield Connect in a 19" rack, follow the instructions supplied with your rack mounting kit.

To install the nShield Connect in a cabinet or a shelf, fit the four self-adhesive rubber feet (supplied with the HSM) to the bottom of the HSM. An x is scored into the chassis at each of the four corners on the bottom of the HSM as a guide to placing the feet.

## Connecting Ethernet and power cables

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

Figure 2. Connecting Ethernet and power cables (nShield Connect back view)



Key	Description
A	Green LED (if on, confirms power is on and unit is not in standby mode).
B	Rocker switch (to turn PSU on and off).
C	Ethernet cable. Two Ethernet ports are available. Port 1 is the left-hand connector when the nShield Connect is viewed from the back.
D	Mains power cables.

The connectors for Ethernet cables and mains power cables are at the rear of the nShield Connect (see Figure 2). Ensure that:

- You connect mains power cables to **both** the PSUs
- The rocker switch for each PSU is in the **on** position.

**Note:** If you connect only one Ethernet cable to the nShield Connect, we recommend that you connect it to Ethernet port 1. This is the left-hand Ethernet connector on the rear of the nShield Connect (shaded in Figure 2).

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

For more information about:

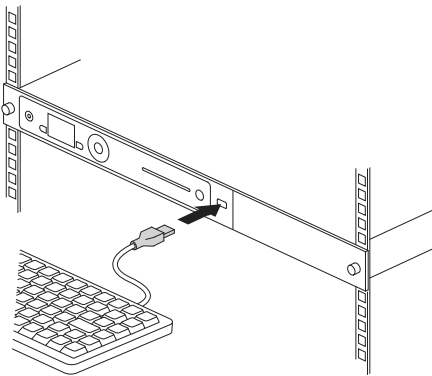
- Audible warnings, see [Audible warning on page 62](#).
- The orange warning LED, see [Orange warning LED on page 62](#).
- Identifying and replacing a faulty PSU, see the *nShield Connect Power Supply Unit Installation Sheet*.



Ensure all power cables are routed to avoid sharp bends, hot surfaces, pinches, and abrasion.

## Connecting the optional USB keyboard

Figure 3. Connecting the optional USB keyboard



Instead of using the controls on the front panel to configure the nShield Connect, you can use a US or UK keyboard (see Figure 3). You might find a keyboard easier for entering dates and IP addresses. You connect the keyboard to the USB connector on the front of the nShield Connect.

### Configuring an nShield Connect for your keyboard type

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

When you have connected a keyboard and configured the nShield Connect for its use, you can enter numbers and characters directly into the display. See the User Guide for more about using a keyboard and keystroke shortcuts.

### Checking the installation

Ensure that:

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

# Chapter 7: Basic nShield Connect and client configuration

This chapter describes the initial nShield Connect and client computer configuration steps. For more about:

- Security World Software installation and options, see [Chapter 4: Installing the software on page 23](#)
- Installing the optional nToken and software, see the *nToken Installation Guide*
- The menu options, see [Top-level menu on page 56](#)
- Advanced nShield Connect and client configuration options, see the User Guide

## About nShield Connect and client configuration

An nShield Connect and a client communicate using their hardserver. These handle secure transactions between the HSM within the Connect and any applications that run on the client. You must configure:

- Each client hardserver to communicate with the hardserver of the nShield Connect that it needs to use.
- The nShield Connect hardserver to communicate with the hardserver of the clients that are allowed to use it.

**Note:** Multiple nShield Connects can be configured to communicate with one client, just as multiple clients can be configured to communicate with one nShield Connect.

## Remote file system (RFS)

Each nShield Connect must have a remote file system (RFS) configured. This normally resides on a client and includes master copies of all the files that the nShield Connect needs. See the User Guide for more about the RFS.



## nShield Connect configuration

The current configuration files for the hardserver of an nShield Connect are stored in its local file system. These files are automatically:

- Updated when the nShield Connect is configured
- Exported to the appropriate RFS directory.

Each nShield Connect in a Security World has separate configuration files on the RFS. See the User Guide for more about nShield Connect configuration files and advanced configuration options.

## Client configuration

The current configuration files for the hardserver of a client are stored in its local file system. You must load the configuration file for it to be used.

See the User Guide for more about client configuration files and advanced configuration options.

**Note:** The following steps assume that you have added the path `%NFAST_HOME%\bin` (Windows) or `/opt/nfast/bin/` (Unix-based systems) to the `PATH` system variable.

## Basic nShield Connect and RFS configuration

After installing the Security World Software and the nShield Connect, you need to do the following:

- Configure the nShield Connect Ethernet interfaces
- Configure the RFS.

You should complete the RFS tasks before :

- Configuring the nShield Connect and client to work together
- Creating a Security World and an Operator Card Set (OCS)  
See the User Guide for more about creating a Security World and the OCS.

## Configuring the Ethernet interfaces - IPv4 and IPv6

An nShield Connect communicates with one or more clients over an Ethernet network. Each client computer has the Security World Software installed. You must supply IP addresses for the nShield Connect and the client. Contact your system administrator for this information if necessary.

You can specify up to two network interfaces for the nShield Connect.

**Note:** If you are configuring both network interfaces, you should **not** use the same subnet for both interfaces.

You can configure the nShield Connect using the front panel **Network config** menu, or by pushing a configuration file to the nShield Connect over the network. The initial set up of the nShield Connect must be done using the front panel. The following can be configured:

- Interface addresses
- Default gateway
- Network routes
- Network speed.

If the nShield Connect is already configured, you can update the displayed values.

If you ever change any of the IP addresses on the nShield Connect, you must update the configuration of all the clients that work with it to reflect the new IP addresses.

**Note:** By default, the hardserver listens on all interfaces. However, you can choose to set specific network interfaces on which the hardserver listens. This may be useful in cases such as if one of the Ethernet interfaces is to be connected to external hosts. See the *User Guide* for more information.

## IPv4 and IPv6

Support for IPv6 is in addition to IPv4. Both Ethernet interfaces can be configured to support:

- IPv4 only
- IPv4 and IPv6 – dual stack
- IPv6 only.

**Note:** Interface#1 is enabled by default and cannot be disabled. Interface #2 is disabled by default and can be enabled and disabled.

## IPv6 Addresses

An IPv4 address is 32 bits long and typically represented as 4 octets, for example 192.168.0.1. An IPv6 address is 128 bits long and is made up of a subnet prefix (n bits long) and an interface ID (128 - n bits long).

An IPv6 address and its associated subnet is typically represented by the notation *ipv6-address/prefix-length*, where:

- *ipv6-address* is an IPv6 address represented in any of the notations described below
- *prefix-length* is a decimal value specifying how many of the leftmost contiguous bits of the address make up the prefix.

The IPv6 address notation mirrors the way subnets are represented in the IPv4 Classless Inter-Domain Routing (CIDR) notation.

## IPv6 Address notation

An nShield Connect will accept an IPv6 address if it is entered in one of the forms shown below and if the address is valid for context in which it is used. There are two conventional forms for representing IPv6 addresses as text strings:

1. The long representation is x:x:x:x:x:x:x, where the x's are fields containing the hexadecimal characters (0 to ffff) for each 16 bits of the address. For example:
  - 1234:2345:3456:4567:5678:6789:789a:89ab
  - 1234:5678:0:0:0:0:9abc:abcd/64
2. If one or more consecutive fields are 0 then they can be replaced by ::. For example:
  - 1234:5678:0:0:0:0:9abc:abcd/64 can be written as 1234:5678::9abc:abcd/64

**Note:** :: can only appear once in an IPv6 address.

**Note:** The nShield Connect front panel only allows lower case hexadecimal characters (a-f) in an IPv6 address.

IPv6 addresses keyed manually on the nShield Connect front panel are validated on entry by the nShield Connect. As well as checking that the format of the address is correct, the nShield Connect also validates that the address entered is valid for the context in which it will be used, see [Acceptable IPv6 Address by Use Case on page 36](#).

If Stateless Address Auto Configuration (SLAAC) is enabled the nShield Connect will automatically form IPv6 addresses from network prefixes contained in Router Advertisements (RAs). RAs are received directly by the nShield Connect Operating System and automatically forms IPv6 addresses by combining the network prefixes contained in the RA with the MAC address of the receiving Ethernet interface. As they are created by the Operating System, SLAAC IPv6 addresses are not subject to the same validation rules as addresses entered via the nShield Connect front panel. If SLAAC is to be used to configure nShield Connect IPv6 addresses in preference to statically entered addresses then network planners must take care to ensure that prefixes advertised to the nShield Connect are of a suitable type, see [Acceptable IPv6 Address by Use Case on page 36](#).

### IPv6 Compliance

A new sub-menu (1-1-1-8 - **Set IPv6 compliance**) has been added to the nShield Connect front panel menu to permit the User to select an IPv6 compliance mode for an nShield Connect. Compliance with **USGv6** or **IPv6 ready** can be selected.

Both these modes change the settings for the nShield Connect firewall so that it will pass-through packets which are discarded in the normal **Default** mode. This behaviour is required for compliance testing but is not recommended for normal use since allowing packets with invalid fields or parameters through the firewall increases the attack surface. When either **USGv6** or **IPv6 ready** are selected, a confirmation message is displayed to reduce the likelihood that they are enabled by accident.

It is recommended that the IPv6 compliance mode is set to **Default** for all normal operations.

### Acceptable IPv6 Address by Use Case

The types of IPv6 which are acceptable as a static address are given in the table below. For examples of valid IPv6 addresses, see [Appendix C: Valid IPv6 Addresses on page 86](#).

Use Case	Acceptable Addrss Type
Static IPv6 Address Entry	<ul style="list-style-type: none"> <li>• Global Unicast</li> <li>• IPv4 Mapped</li> <li>• Local Unicast</li> </ul>
IPv6 Default Gateway	<ul style="list-style-type: none"> <li>• Global Unicast</li> <li>• IPv4 Mapped</li> <li>• Local Unicast</li> <li>• Link-local</li> </ul>

Use Case	Acceptable Addrss Type
IPv6 Route Entry - IP Range	<ul style="list-style-type: none"> <li>• Unknown</li> <li>• Loopback</li> <li>• Global Unicast</li> <li>• IPv4 Mapped</li> <li>• Local Unicast</li> <li>• Link local</li> <li>• Teredo</li> <li>• Benchmarking</li> <li>• Orchid</li> <li>• 6to4</li> <li>• Documentation</li> <li>• Multicast</li> </ul>
IPv6 Route Entry - Gateway	<ul style="list-style-type: none"> <li>• Global Unicast</li> <li>• IPv4 Mapped</li> <li>• Local Unicast</li> <li>• Link-local</li> </ul>
RFS Address	<ul style="list-style-type: none"> <li>• Global Unicast</li> <li>• IPv4 Mapped</li> <li>• Local Unicast</li> <li>• Unspecified address</li> </ul> <p><b>Note:</b> An unspecified address allows all 0s to be used in an IPv6 address.</p>
Client Address	<ul style="list-style-type: none"> <li>• Global Unicast</li> <li>• IPv4 Mapped</li> <li>• Local Unicast</li> </ul>
Push Client Address	<ul style="list-style-type: none"> <li>• Global Unicast</li> <li>• IPv4 Mapped</li> <li>• Local Unicast</li> </ul>
Ping	<ul style="list-style-type: none"> <li>• Unknown</li> <li>• Loopback</li> <li>• Global Unicast</li> <li>• IPv4 Mapped</li> <li>• Local Unicast</li> <li>• Link-local</li> <li>• Teredo</li> <li>• Benchmarking</li> <li>• Orchid</li> <li>• 6to4</li> <li>• Documentaion</li> <li>• Multicast</li> </ul>

Use Case	Acceptable Addrss Type
Traceroute	<ul style="list-style-type: none"> <li>• Unknown</li> <li>• Loopback</li> <li>• Global Unicast</li> <li>• IPv4 Mapped</li> <li>• Local Unicast</li> <li>• Link-local</li> <li>• Teredo</li> <li>• Benchmarking</li> <li>• Orchid</li> <li>• 6to4</li> <li>• Documentation</li> <li>• Multicast</li> </ul>

### Stateless Address Auto Configuration (IPv6 only)

Unlike IPv4, IPv6 is designed to be auto-configuring. SLAAC is an IPv6 mechanism by which IPv6 hosts can configure their IPv6 addresses automatically when connected to an IPv6 network using the Neighbour Discovery Protocol (NDP). Using NDP IPv6 hosts are able to solicit advertisements from on-link routers and use the network prefix(es) contained in the advertisements to generate IPv6 address(es).

SLAAC is disabled by default in an nShield Connect, but can be selectively enabled for each Ethernet interface either using the nShield Connect front panel or by setting the appropriate configuration item and pushing an nShield Connect configuration file.

## Configure Ethernet Interface #1

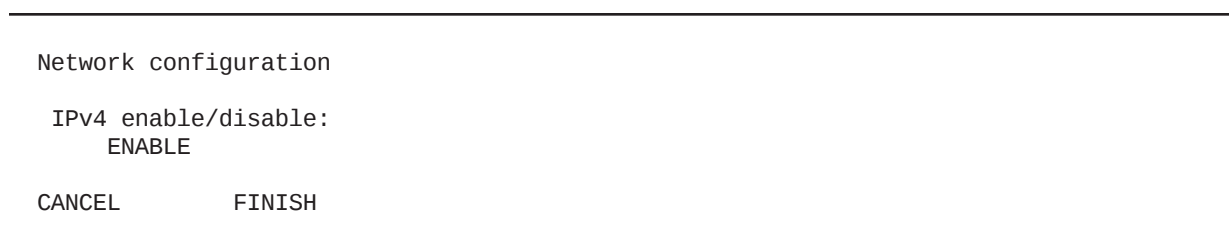
To set up Ethernet interface #1 (default):

### Enable/disable IPv4

To enable/disable IPv4:

1. From the front panel menu, select **System > System configuration > Network config > Set up interface #1 > Configure #1 IPv4 > IPv4 enable/disable**.

The following screen displays:



4. Set the **ENABLE/DISABLE** field to the required option.
5. To accept, press the right-hand navigation button.

## Set up IPv4 static address

To set up IPv4 static address:

1. From the front panel menu, select **System > System configuration > Network config > Set up interface #1 > Configure #1 IPv4 > Static IPv4 address.**

The following screen displays:

---

```

Network configuration

Enter IPv4 address
for interface #1:
  xxx.xxx.xxx.xxx
Enter netmask:
  xxx.xxx.xxx.xxx
CANCEL          NEXT

```

---

4. Set each field of the IP address and netmask for the interface (press the **Select** button to move to the next field).
5. Once all fields have been set, press the right-hand navigation button to continue.
6. To accept the changes, press the right-hand navigation button and then **CONTINUE** to go back to the **Static IPv4 address** menu.

## Enable/disable IPv6

To enable/disable IPv6:

1. From the front panel menu, select **System > System configuration > Network config > Set up interface #1 > Configure #1 IPv6 > IPv6 Enable/Disable.**

The following screen displays:

---

```

Network configuration

IPv6 enable/disable:
  DISABLE

CANCEL          FINISH

```

---

4. Set the **ENABLE/DISABLE** field to the required option.
5. To accept, press the right-hand navigation button.

## Set up IPv6 static address

To set up IPv6 static address:

1. From the front panel menu, select **System > System configuration > Network config > Set up interface #1 > Configure #1 IPv6 > Static IPv6 address > IPv6 address entry.**

The following screen displays:

---

```

Network configuration
Enter IPv6 address
For interface #1:

::

CANCEL          NEXT

```

---

4. Enter the required IPv6 address.
5. When the IPv6 address is correct, press the right-hand navigation button. The following screen displays:

---

```

Network configuration
IPv6 address
xxxx:xxxx:xxxx:xxxx:
  xxxx:xxxx:xxxx:xxxx

Enter prefix length:
          64

BACK          NEXT

```

---

7. When the IPv6 address prefix details are correct, press the right-hand navigation button.
8. You are asked whether you wish to accept the new interface. To accept, press the right-hand navigation button..
9. From the front panel, select **System > System configuration > Network config > Set up interface #1 > Configure #1 IPv6 > Static IPv6 address > Static IPv6 Enab/Dis.** The following screen displays:

---

```

Network configuration

Do you want to enable
a static address? No

CANCEL          FINISH

```

---

12. Select **Yes** and press the right-hand navigation button.
13. A screen will be displayed **Static IPv6 address setup complete**, select **Continue**.

### Set the link speed for Interface #1

To set up the link speed for interface #1:

1. From the front panel menu, select **System > System configuration > Network config > Set up interface #1 > Set link speed for #1**.
2. The following screen displays:

---

Network configuration

Select desired link  
speed:  
auto / 1Gb

CANCEL                      NEXT

---

You can choose from **auto / 1Gb**, **10BaseT**, **10BaseT-FDX**, **100BaseTX**, or **100BaseTX-FDX**.

**Note:** We recommend that you configure your network speed for automatic negotiation, using the **auto / 1Gb** or **auto** option. You will be asked to confirm the changes if **auto / 1Gb** is not selected.

On the nShield Connect, selecting **auto / 1Gb** is the only means of achieving 1Gb link speed.

6. Press the right-hand navigation button and you will be returned to the **Set up interface #1** screen and you can then continue with the configuration.

## Configure Ethernet Interface #2

To set up the Ethernet interface #2, if required:

1. From the front panel menu, select **System > System configuration > Network config > Set up interface #2**.
2. Enter the details for interface #2 in the same manner that you entered the details for interface #1.
3. Once the interface #2 details have been entered you need to explicitly enable interface #2. Select **System > System configuration > Network config > Set up interface #2 > Enable/Disable Int #2**.
4. The following screen displays:

---

Network configuration

Interface #2  
DISABLE

CANCEL                      FINISH

---

6. Select the **ENABLE** option.
7. Press the right-hand navigation button to accept, and a screen similar to that used for interface #1 is displayed.

## Default gateway

### Set default gateway for IPv4

To set a default gateway for IPv4:

1. From the front panel menu, select **System > System configuration > Network config > Set default gateway > IPv4 Gateway**.



The following screen is displayed:

---

```
Gateway configuration
```

```
Enter IPV4 address of
the default gateway:
```

```
0. 0. 0. 0
```

```
CANCEL          NEXT
```

---

4. Enter the IPv4 address of the default gateway.
5. Press the right-hand navigation button **NEXT** and then **FINISH** to accept.

## Set default gateway for IPv6

To set a default gateway for IPv6:

1. From the front panel menu, select **System > System configuration > Network config > Set default gateway > IPv6 gateway**.

The following screen is displayed:

---

```
Gateway configuration
```

```
Enter IPV6 address of
the default gateway:
```

```
::
```

```
CANCEL          NEXT
```

---

Enter the address for the gateway. Press the right-hand navigation button. The following screen is displayed if the address entered was a link-local address:

---

```
Gateway configuration
```

```
Select an interface
for link-local address:
```

```
fe80:xxxx:xxxx:xxxx:
```

```
xxxx:xxxx:xxxx:xxxx
```

```
Interface #1
```

```
CANCEL          NEXT
```

---

Select the interface for the IPv6 gateway. Press the right-hand navigation button to accept.

## Set up Routing

### Set up routing for IPv4

To set a new route entry for IPv4:

- From the front panel menu, select **System > System configuration > Network config > Set up routing > New IPv4 route entry**.  
The following screen is displayed:

---

```

Edit route entry

Enter IP range
and mask length:
0. 0. 0. 0/ 0
Enter the gateway:
0. 0. 0. 0
CANCEL      FINISH

```

---

- Enter the IPv4 address range details for the route. Press the right-hand navigation button to accept.

## Set up routing for IPv6

To set a new route entry for IPv6:

- From the front panel menu, select **System > System configuration > Network config > Set up routing > New IPv6 route entry**.  
The following screen is displayed:

---

```

Edit route entry

Enter the IP range
and prefix length:
::/64

CANCEL      NEXT

```

---

- Enter the IPv6 address range details for the route. Press the right-hand navigation button to accept. The following screen is displayed:

---

```

Edit route entry
xxxx:xxxx:xxxx:xxxx:
  xxxx:xxxx:xxxx:xxxx
  /xxx

Enter the gateway:
::

BACK      NEXT

```

---

- Enter the gateway address; if it is a link local address, the following screen is displayed.

---

```

Edit route entry

Select an interface
for link-local address:
fe80:xxxx:xxxx:xxxx:
xxxx:xxxx:xxxx:xxxx
  Interface #1
  BACK          NEXT

```

---

8. Select the interface for the IPv6 gateway and press the right-hand navigation button to accept.
9. If the new route entry entered for IPv6 is incorrect an error message is displayed on the next screen, select **BACK** to go to the route entry screen. The new IPv6 route entry will need to be entered again.

## Edit route entry

### Edit IPv4 route entry

To edit a route entry for IPv4:

1. From the front panel menu, select **System > System configuration > Network config > Set up routing > Edit route entry**. The following screen is displayed:

---

```

▶ 1. 1. 1. 1/ 1
   3. 3. 3. 3/ 3
   1111:1111:1111:1111:
   1111:1111:1111:1111
   /128

  BACK          SELECT

```

---

4. Select the IPv4 route to be edited. Press the right-hand navigation button. The following screen is displayed:

---

```

Edit route entry

Enter the IP range
and mask length:
1. 1. 1. 1/ 1
Enter the gateway
2. 2. 2. 2
  CANCEL      FINISH

```

---

6. Edit the IPv4 route entry. Press the right-hand navigation button to accept the changes.

### Edit IPv6 route entry

To edit a route entry for IPv6:

- From the front panel menu, select **System > System configuration > Network config > Set up routing > Edit route entry**.

The following screen is displayed:

---

```

Edit route entry
▶ 1. 1. 1. 1/ 1
   3. 3. 3. 3/ 3
   1111:1111:1111:1111:
   1111:1111:1111:1111
   /128

BACK          SELECT

```

---

- Select the IPv6 route to be edited. Press the right-hand navigation button. The following screen is displayed:

---

```

Edit route entry

Enter the IP range
and prefix length:
1111:1111::1111:1111:
 1111:1111:1111:1111/128

CANCEL        NEXT

```

---

- Edit the IPv6 route entry. Press the right-hand navigation button.

---

```

Edit route entry
1111:1111:1111:1111:
 1111:1111:1111:1111/128

Enter the gateway
2222:2222:2222:2222

BACK          NEXT

```

---

- Enter the IPv6 route gateway. If a link-local address is entered for the IPv6 route gateway the screen below will be displayed.

---

```

Edit route entry

Select an interface
for link-local address:
fe80:2222:2222:2222:
2222:2222:2222:2222
  Interface #1
BACK          NEXT

```

---

- Select the interface for the IPv6 gateway. Press the right-hand navigation button to accept.

## Remove route entry

To remove a route entry:

1. From the front panel menu, select **System > System configuration > Network config > Set up routing > Remove route entry**.

The following screen is displayed:

---

```

▶ 1. 1. 1. 1/ 1
   3. 3. 3. 3/ 3
   1111:1111:1111:1111:
   1111:1111:1111:1111
   /128

```

BACK            SELECT

---

4. Select the IPv4/IPv6 route to be removed. Press the right-hand navigation button.
5. The selected route will be displayed. Press the right-hand navigation button to remove the route.

## Enable IPv6 SLAAC

SLAAC can be enabled/disabled independently on each of the two interfaces.

To enable SLAAC:

1. From the front panel menu, select **System > System configuration > Network config > Set up interface #1 > Configure #1 IPv6 > IPv6 SLAAC**.

The following screen is displayed:

---

```

Network configuration
SLAAC State
  Disabled

```

CANCEL            FINISH

---

4. Select the required state and press the right-hand navigation button.
5. The **SLAAC configuration completed OK** screen is displayed. Press the right-hand navigation button to accept.

**Note:** Enable SLAAC for interface #2 in the same manner that you entered the details for interface #1 but select **System > System configuration > Network config > Set up interface #2 > Configure #2 IPv6 > IPv6 SLAAC**.

## Configuring the Remote File System (RFS)

The RFS contains the master copy of the Security World data for backup purposes. The RFS can be located on either a client or another network-accessible computer where the Security World Software is installed. If the RFS is on a client, the same file structure also contains the configuration files for that client.



We recommend that you regularly back up the entire contents of the RFS. Either the `%NFAST_KMDATA%` directory under Windows, or the `kmdata` directory under Unix, is required to restore an nShield Connect or its replacement, to the current state in case of failure.

You can specify a new RFS, and modify or delete an existing RFS configuration. To create or modify a remote file system configuration, specify the IP address of the computer on which the RFS resides.

**Note:** You must have created an RFS on the client computer before you specify the IP address of the client.

See the User Guide for more about the RFS and its contents.

The nShield Connect must be able to connect to TCP port 9004 of the RFS. If necessary, modify the firewall configuration to allow this connection on either the RFS itself or on a router between the RFS and the nShield Connect.

Obtain the following information about the nShield Connect before you set up an RFS for the first time:

- The IP address

The following nShield Connect information can be obtained automatically (or manually):

- The electronic serial number (ESN)
- The hash of the  $\kappa_{\text{NETI}}$  key ( $\text{HK}_{\text{NETI}}$ ). The  $\kappa_{\text{NETI}}$  key authenticates the nShield Connect to clients. It is generated when the nShield Connect is first initialized from factory state.

If your network is secure and you know the IP address of the nShield Connect, you can use the `anonkneti` utility to obtain the ESN and hash of the  $\kappa_{\text{NETI}}$  key by giving the following command on the client computer:

---

```
anonkneti mmm.mmm.mmm.mmm
```

---

In this command, `mmm.mmm.mmm.mmm` is the IP address of the nShield Connect. The command returns output in the following form:

---

```
A285-4F5A-7500 2418ec85c86027eb2d5959fef35edc5e1b3b698f
```

---

In this example output, `A285-4F5A-7500` is the ESN and `2418ec85c86027eb2d5959fef35edc5e1b3b698f` is the hash of the  $\kappa_{\text{NETI}}$  key.

Alternatively, you can find this information on the nShield Connect startup screen. Use the touch wheel to scroll to the appropriate information.

When you have the necessary information, set up an RFS as follows:

1. Prepare the RFS on the client computer (or another appropriate computer) by running the following command on that computer:

---

```
rfs-setup --force mmm.mmm.mmm.mmmEEEE-SSSS-NNNNkeyhash
```

---

In this command:

- `mmm.mmm.mmm.mmm` is the IP address of the nShield Connect
  - `EEEE-SSSS-NNNN` is the ESN of the nShield Connect
  - `keyhash` is the hash of the  $K_{NETI}$  key
4. On the nShield Connect display screen, use the right-hand navigation button to select **System** > **System configuration** > **Remote file system** > **Define IPv4 RFS** and enter the IP address of the client computer on which you set up the RFS.

**Note:** Leave the port number at the default setting of 9004.

To modify an RFS at a later date, select **System configuration** > **Remote file system** > **Define IPv4 RFS**, and then select the required action.

**Note:** You can allow non-nShield Connect hardware security modules to access the remote file system and share Security World and key data that is stored in the `%NFAST_KMDATA%` directory under Windows, or the `kmdata` directory under Unix, in the same way as an nShield Connect. Clients that access data in this way are described as *cooperating clients*. To configure client cooperation, you need to know the details of each client including IP address and ESN.

After you have defined the RFS, the nShield Connect configuration files are exported automatically to it. See the User Guide for more about configuration files.

## Systems configured for Remote Administration

If you are planning to use Remote Administration, you should enable *auto push* on the nShield Connect, once you have configured the RFS.

On the nShield Connect display, use the right-hand navigation button to select **System** > **System configuration** > **Config file options** > **Setup auto push** > **Auto push mode** and select **IPv4**.

Once auto push is enabled, you can complete the configuration steps by editing the configuration files, rather than by using the front panel of the nShield Connect. See the User Guide for more about configuration files.

You do, however, need to set the time and date on the nShield Connect, using the front panel controls. See the User Guide for more information about setting the time and date.

## Basic configuration of the client to use the nShield Connect

### Client configuration utilities

The following client configuration utilities are available:

Utility	Description
<code>nethsmenrol1</code>	Used to configure the client to communicate with the nShield Connect.
<code>config-serverstartup</code>	Used to configure the hardware server of the client to enable TCP sockets.

## nethsmenroll

The `nethsmenroll` command-line utility is used to edit the configuration file of the client hardserver to add an nShield Connect. If the `ESN` and `HKNETI` are not specified, `nethsmenroll` attempts to contact the nShield Connect to determine what they are, and requests confirmation.

Usage:

---

```
nethsmenroll [Options] --privileged <nShield Connect IP><nShield Connect ESN><nShield Connect KNETI HASH>
```

---

Options:

<code>-m, --module=MODULE</code>	Specifies the local module number that should be used (default is 0 for dynamic configuration by hardserver).
<code>-p, --privileged</code>	Makes the hardserver request a privileged connection to the nShield Connect (default <code>unprivileged</code> ).
<code>-r, --remove</code>	Removes the configuration of the specified nShield Connect.
<code>-f, --force</code>	Forces reconfiguration of an nShield Connect already known.
<code>--no-hkneti-confirmation</code>	Does not request confirmation when automatically determining the nShield Connect's <code>ESN</code> and <code>HKNETI</code> . <b>Note:</b> CAUTION! This option is potentially insecure and should only be used on secure networks where there is no possibility of a man-in-the-middle attack.
<code>-v, --verify-nethsm-details</code>	When the <code>ESN</code> and <code>HKNETI</code> have been provided on the command line, verifies that the selected HSM is online, reachable and matches those details.
<code>-P, --port=PORT</code>	Specifies the port to use when connecting to the given nShield Connect (default <code>9004</code> ).
<code>-n, --ntoken-esn=ESN</code>	Specifies the <code>ESN</code> of the LOCAL nToken that should be used when connecting to the nShield Connect (default <code>empty</code> , i.e. no nToken authentication used)

## config-serverstartup

The `config-serverstartup` command-line utility automatically edits the `[server_startup]` section in the local hardserver configuration file in order to enable TCP ports for Java and KeySafe. Any fields for which values are not specified remain unchanged. After making any changes you are prompted to restart the hardserver.

Run `config-serverstartup` using the following commands:

---

```
config-serverstartup [OPTIONS]
```

---

For more information about the options available to use with `config-serverstartup`, run the command:



```
config-serverstartup --help
```

---

## Configuring a client to communicate through an nToken

You can configure a client to use its nToken to communicate with an nShield Connect, if it has one installed. When this happens, the nShield Connect:

- Examines the IP address of the client
- Requires the client to identify itself using a signing key

**Note:** If an nToken is installed in a client, it can be used to both generate and protect a key that is then used for the impath communication between the nShield Connect and the client. A strongly protected key is used at both ends of the impath as a result.

## Enrolling the client from the command line

Complete the following steps to initially configure a client computer to communicate with and use an nShield Connect. See [Basic nShield Connect and client configuration on page 33](#) for more about the available options.

Do the following:

1. On the client, open a command line window, and run the command:

---

```
nethsmenroll --help
```

---

3. To retrieve the **ESN** and **HKNETI** of the nShield Connect, run the command:

---

```
anonkneti <Unit IP>
```

---

The following is an example of the output:

---

```
3138-147F-2D64 691be427bb125f38768638a18bfd2eab75623320
```

---

If the **ESN** and **HKNETI** are not specified, **nethsmenroll** attempts to contact the nShield Connect to determine what they are, and requests confirmation.

8. Do one of the following:

a. If you are enrolling a client *with* an nToken installed, run the command:

```
nethsmenroll --ntoken-esn <nToken ESN> [Options] --privileged <Unit IP> <Unit ESN> <Unit KNETI HASH>
```

---

c. If you are enrolling a client *without* an nToken installed, run the command:

```
nethsmenroll [Options] --privileged < Unit IP> < Unit ESN> < Unit KNETI HASH>
```

---

The following is an example of the output:

```
OK configuring hardserver's nethsm imports.
```

---

## Configure the TCP sockets on the client for Java applications (for example, KeySafe)

Do the following:

1. Run the command:

```
config-serverstartup --enable-tcp --enable-privileged-tcp
```

---

3. Do one of the following to stop and restart the hardserver, according to your operating system:

a. **Windows:**

```
net stop "nfast server"  
net start "nfast server"
```

---

c. **Unix-based:**

```
/opt/nfast/sbin/init.d-ncipher restart
```

---

4. Test the completed installation by running the command:

```
enquiry
```

---

See [Enquiry utility on page 60](#) for an example of the output that the **enquiry** utility generates.

## Basic configuration of an nShield Connect to use a client

Do the following:

1. On the nShield Connect front panel, use the right-hand navigation button to select **System > System configuration > Client config > New IPv4 client**.

The following screen displays:

---

```
Client configuration
Please enter your
client IPv4 Address
  0. 0. 0. 0
CANCEL          NEXT
```

---

4. Enter the IP address of the client, and press the right-hand navigation button. You are asked to choose the permissions for the client:

---

```
Client configuration
Please choose the
client permissions
Unprivileged
BACK          NEXT
```

---

7. Use the touch wheel to display the type of connection between the nShield Connect and the client. The following options are available:

Option	Description
Unprivileged	Privileged connections are never allowed.
Priv. on low ports	Privileged connections are allowed only from ports numbered less than 1024. These ports are reserved for use by root on Unix-based systems.
Priv. on any ports	Privileged connections are allowed on all ports.



A privileged connection is required to administer the nShield Connect, for example to initialize a Security World. If privileged connections are allowed, the client can issue commands (such as clearing the nShield Connect) which interfere with the normal operation of the nShield Connect. We recommend that you allow only unprivileged connections unless you are performing administrative tasks.

10. When you have selected a connection option, press the right-hand navigation button. The following screen is displayed:

---

```

Client configuration
This client is not
configured to use an
nToken. Do you want to
enroll with an nToken?
      NO
BACK          NEXT

```

---

The next steps in the configuration process vary slightly depending on whether the client uses an nToken to communicate with the nShield Connect, or not.

13. Do one of the following:

- a. To enroll the client without nToken authentication, select **No** and press the right-hand navigation button. The unit displays a message reporting that the client has been configured.
- b. Press the right-hand navigation button again.

or:

- a. To enroll the client with nToken authentication, you must first confirm the nToken authentication key. On the client, open a command line window, and run the command:

---

```
ntokenenroll -H
```

---

The following is an example of the output:

---

```

nToken module #1
  nToken ESN:      3138-147F-2D64
  nToken key hash: 691be427bb125f387686
                  38a18bfd2eab75623320

```

---

- e. Ensure that you write down the hash or have it otherwise available for the next steps.
- f. On the nShield Connect, enter the number of the port on which the client is listening and press the right-hand navigation button. (The default port is 9004.)

The following is an example of the information displayed by the nShield Connect. This identifies the client by its ESN and displays the reported key hash:

---

```

Client nnnnnnnnn reported the key hash:
691be427bb125f387686
38a18bfd2eab75623320
Is this EXACTLY right?
      Yes  No
CANCEL          FINISH

```

---

- i. Compare the hash displayed by the nShield Connect with the nToken key hash returned by `ntokenenroll`.

- j. If there is an exact match, select **Yes** and then press the right-hand navigation button to configure the client.
- k. The unit displays a message reporting that the client has been configured. Press the right-hand navigation button again.

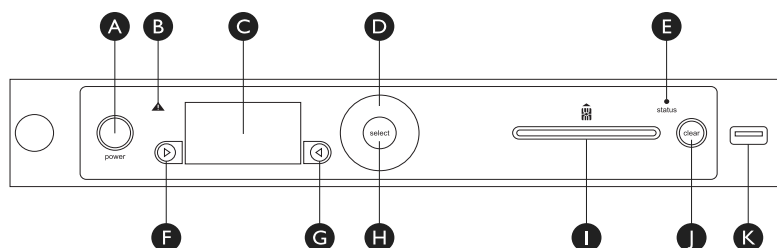
See the User Guide for more about modifying or deleting an existing client, configuring multiple clients, client licenses, configuring an nShield Connect to use a client with configuration files and auto push, and advanced configuration options.

## Using a Security World

See the User Guide for more about creating a Security World or loading an existing one.

# Chapter 8: Front panel controls

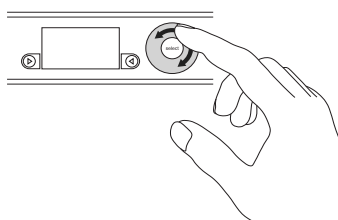
Figure 4. Front panel controls



Key	Description
A	Power button
B	Warning LED (orange)
C	Display screen
D	Touch wheel
E	Status indicator LED (blue)
F	Display navigation button (left)
G	Display navigation button (right)
H	<b>Select</b> button
I	Slot for smart cards
J	Clear button
K	USB connector

For more information about the user interface, including the front panel controls, see the *nShield Connect User Guide*.

Figure 5. Touch wheel



Use the touch wheel to change values or move the cursor on the display screen. To confirm a value, press the **Select** button.

# Chapter 9: Top-level menu

The tables below list all the menu options.

**Note:** If you select an option, the module displays the menu options in the level below. If you cancel a selected option, you return to level above.

Top-level menu	Submenus
1 System	1-1 System configuration
	1-2 System information
	1-3 Login settings
	1-4 Upgrade system
	1-5 Factory state
	1-6 Shutdown/Reboot
2 HSM	2-1 HSM information
	2-2 HSM reset
	2-3 HSM feature enable
	2-4 Set HSM mode
3 Security World mgmt	3-1 Display World info
	3-2 Module initialization
	3-3 RFS operations
	3-4 Admin operations
	3-5 Cardset operations
	3-6 Card operations
	3-7 Keys
	3-8 Set up remote slots *
4 payShield *	
5 CodeSafe *	

\* Submenus depend on the settings of the module.

# 1 System

System menu	Submenus
1-1 System configuration	1-1-1 Network config
	<ul style="list-style-type: none"> <li>• 1-1-1-1 Set up interface #1</li> <li>• 1-1-1-2 Set up interface #2</li> <li>• 1-1-1-3 Set default gateway</li> <li>• 1-1-1-4 Set up routing *</li> <li>• 1-1-1-5 Show routing table</li> <li>• 1-1-1-6 Ping remote host</li> <li>• 1-1-1-7 Trace route to host</li> <li>• 1-1-1-8 Set IPv6 compliance</li> </ul>
	1-1-2 Hardserver config
	1-1-3 Remote file system
	1-1-4 Client config *
	1-1-5 Resilience config
	1-1-6 Config file options
	<ul style="list-style-type: none"> <li>• 1-1-6-1 Fetch configuration</li> <li>• 1-1-6-2 Setup auto push</li> </ul>
	1-1-7 Log config
	1-1-8 Date/time setting
	1-1-9 Keyboard layout
	<ul style="list-style-type: none"> <li>• 1-1-9-1 UK keyboard</li> <li>• 1-1-9-2 US keyboard</li> </ul>
1-1-10 Tamper config	
1-1-11 Default config	
1-1-12 Remote configuration options	
<ul style="list-style-type: none"> <li>• 1-1-12-1 Remote mode change</li> </ul>	



System menu	Submenus
1-2 System information	1-2-1 View system log 1-2-2 View hardserver log 1-2-3 View IPv6 addresses 1-2-4 Display tasks 1-2-5 Component versions 1-2-6 View h/w diagnostics <ul style="list-style-type: none"> <li>• 1-2-6-1 View power readings</li> <li>• 1-2-6-2 View other readings</li> <li>• 1-2-6-3 Critical Errors</li> </ul> 1-2-7 View tamper log 1-2-8 View unit id
1-3 Login settings	1-3-1 Enable UI Lockout <ul style="list-style-type: none"> <li>• 1-3-1-1 UI Lockout with OCS</li> <li>• 1-3-1-2 UI Lockout w/out OCS</li> </ul> 1-3-2 Power switch lockout 1-3-3 Login control status
1-4 Upgrade system	
1-5 Factory state	
1-6 Shutdown/Reboot	1-6-1 Shutdown 1-6-2 Reboot

\* Submenus depend on the settings of the module.

## 2 HSM

HSM menu	Submenus
2-1 HSM information	2-1-1 Display details 2-1-2 Display secure RTC 2-1-3 Speed test 2-1-4 Display statistics
2-2 HSM reset	
2-3 HSM feature enable	2-3-1 Read FEM from card 2-3-2 Read from a file 2-3-3 View current state 2-3-4 Write state to file
2-4 Set HSM mode	2-4-1 Operational 2-4-2 Initialization

### 3 Security World mgmt

Security World mgmt menu	Submenus
3-1 Display World info	
3-2 Module initialization	<ul style="list-style-type: none"> <li>3-2-1 New Security World</li> <li>3-2-2 Load Security World</li> <li>3-2-3 Erase Security World</li> </ul>
3-3 RFS operations	<ul style="list-style-type: none"> <li>3-3-1 Update World files</li> <li>3-3-2 Remove RFS lock</li> </ul>
3-4 Admin operations	<ul style="list-style-type: none"> <li>3-4-1 Replace ACS</li> <li>3-4-2 Recover keys</li> <li>3-4-3 Recover PIN</li> <li>3-4-4 Set secure RTC</li> </ul>
3-5 Cardset operations	<ul style="list-style-type: none"> <li>3-5-1 Create OCS</li> <li>3-5-2 List cardsets</li> </ul>
3-6 Card operations	<ul style="list-style-type: none"> <li>3-6-1 Card details</li> <li>3-6-2 Check PIN</li> <li>3-6-3 Change PIN</li> <li>3-6-4 Erase card</li> </ul>
3-7 Keys	<ul style="list-style-type: none"> <li>3-7-1 List keys</li> <li>3-7-2 Verify key ACLs</li> </ul>
3-8 Set up remote slots *	
3-9 Set up dynamic slots	<ul style="list-style-type: none"> <li>3-9-1 Dynamic Slots</li> <li>3-9-2 Slot mapping</li> </ul>

\* Submenus depend on the settings of the module.

# Chapter 10: Troubleshooting

This chapter describes what to do if you have an issue with your HSM, or your Security World Software.

## Checking operational status

Use the following methods to check the operational status of the module.

### Enquiry utility

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

- `C:\Program Files\nCipher\nfast` for Windows
- `/opt/nfast` for Unix-based systems

If the module is working correctly, the `enquiry` utility returns the message:

---

```
Server:
enquiry reply flags none
enquiry reply level Six
...
Module ##:
...
mode           operational
version       #.##.#
```

---

If the output from the `enquiry` utility does not show `mode operational`, you can use the Status LED to discover the status of the module.

## Status LED

The blue Status LED indicates the operational status of the module.

Status LED	Description
Off.	<p><b>Status: Power off or Standby mode</b></p> <p>There is either no power supply to the module or the module is in Standby mode. If you suspect that there is no power supply, check that the module is properly connected and switched on.</p> <p>If you believe the module's power supply unit has failed, contact Support.</p>
On, occasionally blinks off.	<p><b>Status: Operational mode</b></p> <p>The module is in Operational mode and accepting commands. The more frequently the Status LED blinks off, the greater the load on the module.</p>
Flashes two short pulses, followed by a short pause.	<p><b>Status: Initialization mode</b></p> <p>Existing Security World data on the module has been erased.</p> <p>The module is automatically placed in Initialization mode after a Security World is created. For more information, see the <i>nShield Connect User Guide</i>.</p>
Flashes two long pulses followed by a pause.	<p><b>Status: Maintenance mode</b></p> <p>Used for reprogramming the module with new firmware.</p> <p>The module only goes into Maintenance mode during a software upgrade.</p>
Flashes SOS, the Morse code distress code (three short pulses, three long pulses, three short pulses). After flashing SOS, the Status LED flashes a Morse code letter which identifies the error.	<p><b>Status: Error mode</b></p> <p>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.</p> <p>For internal security modules running firmware 2.61.2 and above, the error code is also reported by the <b>enquiry</b> utility in the <b>hardware status field</b> of the <b>Module</b> and under <b>hardware errors</b> in the hardserver log.</p> <p>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.</p> <p>For information about error codes, see the User Guide.</p>

## Audible warning

An audible warning sounds for some critical errors relating to the PSUs on the module. The orange warning LED (see [Orange warning LED on page 62](#)) accompanies the audible warning.

The warning sounds when only one of the two PSUs is powered and turned on. Check that:

- The rocker switch on both PSUs is in the **on** position
- Both PSUs are connected to the mains supply

If the audible warning continues, there might be a fault with one or both PSUs. Before investigating further, switch off the audible alarm by navigating to the **1-2-5-3 Critical Errors** screen. The orange warning LED remains on until you resolve the issue.

For more information about identifying and replacing a failed PSU, see the *nShield Connect Power Supply Unit Installation Sheet*.

## Orange warning LED

If the orange warning LED (see [Orange warning LED on page 62](#)) is on, the module has encountered a critical error (for example, overheating or PSU failure) that may require immediate action. To find the cause of a critical error, navigate to **System information > View h/w diagnostics > Critical Errors**.

## Checking the physical security of the module

The physical security measures implemented on the module include tamper detection. This warns you of tampering in an operational environment. For more information about tamper detection, including the tamper warning messages, see the *nShield Connect Physical Security Checklist* or the *nShield Connect User Guide*.

## Display screen

When the module is in Maintenance or Initialization mode, there is a color-coded footer at the bottom of the display screen. There is no footer when the module is in Operational mode.

Footer color	Text in footer	Meaning
Yellow	Initialization	The system is rebooting or waiting for an Administrator Card to be inserted.
Blue	Maintenance	An administrative task is being performed. This mode is only entered during firmware upgrades.
Red	HSM Failed	The internal module has failed. See <a href="#">Orange warning LED on page 62</a> for more information.



Do not interrupt power to the module during a firmware upgrade.

**Note:** The blue Status LED flashes to indicate the status of the internal security module.

## Power button

The Power button, in combination with the display screen, indicates the general status of the module.

**Note:** The display screen turns off automatically if the front panel buttons are inactive for more than three minutes. Use the touch wheel to turn the display screen back on.

Power button	Display screen	Status
On	On, displaying menus and dialogs	The module is operational.
On	On, displaying messages but not displaying labels for the navigation buttons	The module is running an upgrade. A color-coded footer indicates the specific status: yellow for initialization, red (maintenance) for upgrade.
On, flashes occasionally	On, displaying messages but not displaying labels for the navigation buttons	The module is performing start-up.
Mostly off, flashes occasionally	Off	The module is in Standby mode (that is, it has been powered down from the front panel using the Power button). Press the Power button to turn it on.
Flashes regularly	On, with "Critical Error" message	The module is unable to start-up or has failed. The error message describes the problem. If you can remedy the problem, do so, and press the Power button to restart the module. Otherwise, contact Support.
Flashes irregularly	Off	A low-level critical error has occurred.

## Ethernet LEDs

There are four Ethernet LEDs, two for each of the two Ethernet ports on the module. The Ethernet LEDs indicate the status of the connection with other Ethernet devices.

Ethernet LEDs	Status
Flashes regularly	The status of the Ethernet link is currently unknown (the Ethernet LEDs flash when the module is powering up).
Off	There is no Ethernet link. The Ethernet cable is either not connected to the module or the cable is not connected to a functioning Ethernet device.
On, green only	Indicates a 10Mb or 100Mb Ethernet link.
On, green and orange	Indicates a 1Gb Ethernet link.

## Module overheating

If the internal module of the nShield Connect exceeds the safe operating temperature, the unit stops operating and displays the `sos-T` error message on the Status LED. See [Status LED on page 61](#) for details of the `sos-T` error message.

## Log messages for the module

To view log messages from the main menu of the module:

1. Select **System > System information**
2. Select either:
  - **View system log**
  - **View hardserver log**

The client can store logs, and can configure them to contain different types of message.

## 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
```

---

## Notice

This type of message is sent for information only:

---

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

---

## 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
```

---

---

## 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.

## 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.

## 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 *nShield Connect User Guide*. If reinstallation does not solve the problem, contact Support.

## 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.



## Utility error messages

This type of message might indicate an error status when you run a command line utility.

### **BadTokenData error in nShield modules**

Some nShield modules are equipped with a rechargeable backup battery for maintaining Real Time Clock (RTC) operation when the module is powered down. This battery normally lasts for up to 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.

# Chapter 11: nShield Connect maintenance


The nShield Connect contains only two user-replaceable parts:


- The PSUs
- The fan tray module

Replacing a PSU or fan tray module does not affect FIPS 140-2 validations for the nShield Connect, or result in a tamper event. However, in the very rare event that a PSU or fan tray module requires replacement, contact Support before carrying out the replacement procedure.

 Do not remove the fan tray for more than 30 minutes, otherwise a tamper event will occur.

For more information about replacing either a PSU or the fan tray module, see the Installation Sheet that accompanies the replacement part.

 Breaking the security seal or dismantling the nShield Connect voids your warranty cover, and any existing maintenance and support agreements.

 Mains power plugs on UK cordsets contain a 5A fuse (BS1362). Only replace with the same type and rating of fuse. If a replacement fuse fails immediately, contact Support. Do **not** replace with a higher value fuse.

## Flash testing the module

The module is designed to comply with IEC/EN 60950-1 but should be tested only by trained safety professionals. Because the module is fitted with radio frequency interference suppressors, it is recommended that only a DC test be performed.

 Repeated application of the flash test can damage safety insulation.

# Chapter 12: Approved accessories

The following parts can be ordered with the HSM or separately.

Part	Part number	Comments
Slide rail assembly	AC2050	Optional slide rail assembly and fixing kit. For details of contents, see the <i>nShield Connect Slide Rails Instructions</i> .
USB keyboard	M-030099-L	For more information about using a USB keyboard with the HSM, see <i>Connecting the optional USB keyboard</i> on page 32.
Replacement fan tray module	AC2064	Includes installation instructions.
Replacement PSU	AC2057	Includes installation instructions.

If you have an enquiry about any of the parts listed, contact Support.

# 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 other components or any key data and Security World data that you have created. However, in Unix environments, a manual installation using `.tar` files *does* overwrite existing data and directories.

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

**Note:** 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.

**Note:** 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.

**Note:** 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.

**Note:** 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.

## 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.

---

## Uninstalling Unix software

### 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.

**Note:** 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.

---

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

**Note:** 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.

## 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 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.

**Note:** 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.

## 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`.

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

---

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

---

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

---

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

---

**Note:** Deleting all the files and subdirectories in `/opt/nfast` also deletes the `/opt/nfast/kmdata` directory. To be able to restore an existing Security World after deleting all the files in `/opt/nfast`, ensure you have made a backup of the `/opt/nfast/kmdata` directory in a safe location before deleting the original.

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

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

- Unless needed for a subsequent installation, remove the user `nfast` and, if it exists, the user `ncsnmpd`:

- Open the file `/etc/group` with a text editor.
- Remove the line that begins with the form:

---

```
nfast:x:n
```

---

In this line, *n* is an integer.

- Open the file `/etc/passwd` with a text editor.
- Remove the line that begins with the form:

---

```
nfast:x:...
```

---

- 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 23](#).

nCipher supply the hardware server 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.

## 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:

### Component bundles

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

## Individual components

Unix Package Description (Windows and Unix)	
	nCipher CAPI-NG providers and tools - Windows only
hwcrhk	Crypto Hardware Interface (CHIL) plugin
jceesp	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

## CipherTools installation media

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

### Component bundles

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

## 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
jceesp	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

## CodeSafe installation media

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

### Component bundles

Unix Package	Description (Windows and Unix)	Contents of bundle
hwsp	Hardware Support (mandatory)	See <i>Hardware support</i>
ctl1s	Core Tools (recommended)	See <i>Core tools</i>
javasp	Java Support (including KeySafe)	See <i>Java Support (including KeySafe)</i>
csd	CodeSafe Developer	See <i>CipherTools Developer</i>
jd	Java Developer	See <i>Java Developer</i>
nhfw	nShield Connect firmware files	See <i>nShield Connect firmware files</i>
dsserv	Remote Administration Service (optional)	See <i>Remote Administration Service</i>
rat1s	Remote Administration Client (optional) - Windows and Linux only	See <i>Remote Administration Client</i>

## 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
jceesp	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

## 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.

### 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.

### 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

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

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

**Note:** 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.

## Java Support (including KeySafe)

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

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

## **Remote Administration Service**

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

## **Remote Administration Client**

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

## **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.

## **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.

## CipherTools Developer

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

### Unix Package Description (Windows and Unix)

<b>emvspj</b>	<b>JNI library for payShield Java</b>
<b>emvsp</b>	<b>payShield developer library</b>
<b>hwcrhk</b>	<b>Crypto Hardware Interface (CHIL) dev kit</b>
<b>nflibs</b>	<b>nCipher libraries and headers, and example C source for utility functions</b>
<b>nfuser</b>	<b>nCore &amp; KM tools and example source</b>
<b>pkcs11</b>	<b>nFast PKCS#11 developer's library</b>
<b>sworld</b>	<b>Key Management C library developers kit</b>
<b>tclsrc</b>	<b>Tcl run time - Headers and Libraries</b>
<b>cutils</b>	<b>C utilities library</b>
<b>nflog</b>	<b>Logging library</b>
<b>hilibs</b>	<b>GS libs &amp; headers</b>
<b>pysrc</b>	<b>Python source for developers</b>
<b>nfp</b>	<b>nFPython header files</b>



## CodeSafe Developer

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

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

## Java Developer

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

### Unix Package Description (Windows and Unix)

<code>jcecp</code>	Java Key Management developer
<code>jutils</code>	Java utilities source and javadocs
<code>kmjava</code>	Java Key Management developer
<code>nfjava</code>	Java Generic Stub examples & javadoc

## 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 `nC4nn2` or `Bn1 nnn`, install the **Prebuilt arm-gcc for Codesafe/C** component.
- If your module has a part code of the form `nC4nn3`, `Bn2nnn`, `BN2nnn(-E)`, or `NH2nnn`, 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.

## KeySafe

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

### 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**

### 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, 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/resources/integration-guides>.

### 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.

**Note:** Security World Software supports OpenSSL 1.0.1g and later.

## 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.

## 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: Valid IPv6 Addresses

This appendix provides a list of valid IPv6 addresses for each of the types of addresses recognized by the system. For information on setting up IPv6 addresses, see [Acceptable IPv6 Address by Use Case on page 36](#).

Address type	Address Range (inclusive)		Example
	From	To	
Unspecified	::	::	::
Loopback	::1	::1	::1
IPv4 Mapped	::ffff:0:0	::ffff:ffff:ffff	::ffff:c000:22f
	::ffff.0.0.0.0	::ffff:255.255.255.255	::ffff:192.0.2.47
Local Unicast	fc00::	fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	fd8:f53b:82e4::53
Link-local	fe80::	febf:ffff:ffff:ffff:ffff:ffff:ffff:ffff	fe80::200:5aee:feaa:20a2
Site-local (deprecated)	fec0::	feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	fec0::100:abc:22
Teredo	2001::	2001:0:ffff:ffff:ffff:ffff:ffff:ffff	2001:0:4136:e378:8000:63bf:3fff:fd2
Benchmarking	2001:2::	2001:2:0:ffff:ffff:ffff:ffff:ffff	2001:2:0:6c::430
Orchid	2001:10::	2001:1f:ffff:ffff:ffff:ffff:ffff:ffff	2001:10:240:ab::a
6to4	2002::	2002:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2002:cb0a:3cdd:1::1
Documentation	2001:db8::	2001:db8:ffff:ffff:ffff:ffff:ffff:ffff	2001:db8:8:4::2
Global Unicast	2000::	3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	20ab:45:fa::adb5
Multicast	ff00::	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	ff01::2

**Note:** The available addresses in the Global Unicast range are not contiguous.