nShield Security World

# nShield Connect v13.4.5 Install Guide

17 October 2024

# Table of Contents

# 1. Introduction

The Entrust 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 HSMs on the network, as well as locally installed HSMs.

## 1.1. About this guide

This guide includes:

- Installing the Security World Software. See Installing the software.
- Physically installing an nShield Connect. See Installing an HSM.
- Configuring an nShield Connect and client. See Basic HSM, RFS and client configuration.
- The nShield Connect front panel controls. See Front panel controls.
- The top-level menu of an nShield Connect. See Top-level menu.
- Troubleshooting information. See Troubleshooting.
- nShield Connect maintenance. See HSM maintenance.
- Accessories. See Approved accessories.
- Instructions to uninstall existing software. See Uninstalling existing software.
- Software components and bundles. See Software packages on the Security World software installation media.

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 Entrust nShield products with third-party enterprise applications, see https://www.entrust.com/digital-security/hsm.

## 1.2. Model numbers

Model numbering conventions are used to distinguish different nShield hardware security

devices.

| 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 Medium |
| NH2075-H | nShield Connect XC High |
| NH2082 | nShield Connect XC SCAP |
| NH2089-B | nShield Connect XC Base - Serial Console |
| NH2089-M | nShield Connect XC Mid - Serial Console |
| NH2089-H | nShield Connect XC High - Serial Console |
| NH3003-B | nShield Connect CLX Base - Serial Console |
| NH3003-M | nShield Connect CLX Mid - Serial Console |
| NH3003-H | nShield Connect CLX High - Serial Console |

## 1.3. Power and safety requirements

The module draws up to 220 watts:

- Voltage: 100 VAC -240 VAC

- Current: 2.0 A - 1.0 A

- Frequency: 50 Hz - 60 Hz.

> The module PSUs are compatible with international mains voltage supplies.

## 1.4. Terminology

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

## 1.5. 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).

## 1.6. Weight and Dimensions

Weight:  11.5kg

Dimensions: 43.4mm x 430mm x 690mm

> ℹ️ 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.

## 1.7. 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.

### 1.7.1. Temperature and humidity recommendations

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

| Environmental conditions | Operating range (Min. \| Max.) | | Comments |
|---|---|---|---|
| Operating temperature | 5 °C | 35 °C | - |
| Storage temperature | -20 °C | 70 °C | - |
| Operating humidity | 10 % | 85 % | Relative. Non-condensing at 35 °C. |
| Storage humidity | 0 % | 95 % | Relative. Non-condensing at 35 °C. |
| Altitude | -100 m | 2000 m | Above Mean Sea Level (AMSL) |

## 1.7.2. Cooling requirements

Adequate cooling of your module is essential for trouble-free operation and a long operational life. During operation, you can use the 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). If the whole nShield Connect overheats, the orange warning LED on the front panel illuminates (see Orange warning LED) and a critical error message is shown on the display.

## 1.8. Physical location considerations

Entrust nShield HSMs are certified to NIST FIPS 140 Level 2 and 3. In addition to the intrinsic protection provided by an nShield HSM, customers must exercise due diligence to ensure that the environment within which the nShield HSMs are deployed is configured properly and is regularly examined as part of a comprehensive risk mitigation program to assess both logical and physical threats. Applications running in the environment shall be authenticated to ensure their legitimacy and to thwart possible proliferation of malware that could infiltrate these as they access the HSMs' cryptographic services. The deployed environment must adopt 'defense in depth' measures and carefully consider the physical location to prevent detection of electromagnetic emanations that might otherwise inadvertently disclose cryptographic material.

# 2. Recycling and disposal information

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

# 3. Before you install the software

Before you install the software, you should:

- If required, install an optional nToken in the client computer, see *nToken Installation Guide* for more information about the installation steps.

- Uninstall any older versions of Security World Software. See Uninstalling existing software.

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

- Complete any other necessary preparatory tasks, as described in Preparatory tasks before installing software.

## 3.1. 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.

### 3.1.1. Windows

Adjust your computer's power saving setting to prevent sleep mode.

#### 3.1.1.1. Install Microsoft security updates

Make sure that you have installed the latest Microsoft security updates. Information about Microsoft security updates is available from http://www.microsoft.com/security/.

### 3.1.2. Linux

#### 3.1.2.1. Install operating environment patches

Make sure that you have installed:

- kernel packages like `gcc`, `kernel-headers`, `kernel-devel`
- the latest recommended patches for your environment in general

See the documentation supplied with your operating environment for information.

---

### 3.1.2.2. Users and groups

The installer automatically creates the following group and users if they do not exist. If you wish to create them manually, you should do so before running the installer.

Create the following, as required:

- The `nfast` user in the `nfast` group, using `/opt/nfast` as the home directory.
- If you are installing snmp, the `ncsnmpd` user in the `ncsnmpd` group, using `/opt/nfast` as the home directory.
- If you are installing the Remote Administration Service, the `raserv` user in the `raserv` group, using `/opt/nfast` as the home directory.

## 3.1.3. All environments

### 3.1.3.1. Install Java with any necessary patches

The following versions of Java have been tested to work with, and are supported by, your nShield Security World Software:

- Java7 (or Java 1.7x)
- Java8 (or Java 1.8x)
- Java11.

Entrust recommends that you ensure Java is installed before you install the Security World Software. The Java executable must be on your system path.

If you can do so, please use the latest Java version currently supported by Entrust that is compatible with your requirements. Java versions before those shown are no longer supported. If you are maintaining older Java versions for legacy reasons, and need compatibility with current nShield software, please contact Entrust nShield Support, https://nshieldsupport.entrust.com.

To install Java you may need installation packages specific to your operating system, which may depend on other pre-installed packages to be able to work.

Suggested links from which you may download Java software as appropriate for your operating system:

- http://www.oracle.com/technetwork/java/index.html
- http://www.oracle.com/technetwork/java/all-142825.html

  > You must have Java installed to use KeySafe.

---

### 3.1.3.2. Identify software components to be installed

Entrust supply standard component bundles that contain many of the necessary components for your installation and, in addition, individual components for use with supported applications. To be sure that all component dependencies are satisfied, you can install either:

- All the software components supplied.
- Only the software components you require.

During the installation process, you are asked to choose which bundles and components to install. Your choice depends on a number of considerations, including:

- The types of application that are to use the module.
- The amount of disc space available for the installation.
- Your company's policy on installing software. For example, although it may be simpler to choose all software components, your company may have a policy of not installing any software that is not required.

> On Windows, the `nShield Hardware Support bundle` and the `nShield Core Tools bundle` are mandatory, and are always installed.

The `Core Tools bundle` contains all the Security World Software command-line utilities, including:

- `generatekey`.
- Low level utilities.
- Test programs.

The `Core Tools bundle` includes the `Tcl run time` component that installs a run-time Tcl installation within the nCipher directories. This is used by the tools for creating the Security World and by KeySafe. This does not affect any other installation of Tcl on your computer.

You need to install the Remote Administration Service component if you require remote administration functionality. See Preparatory tasks before installing software and the *nShield Connect User Guide* for more about the Remote Administration Service.

> Always install all the nShield components you need in a single installation process to avoid subsequent issues should you wish to uninstall. You should not, for example, install the Remote Administration Service from the Security World installation media, then later install the Remote Administration Client from the client installation media.

Ensure that you have identified any optional components that you require before you install

the Security World Software. See Software packages on the Security World software installation media for more about optional components.

## 3.2. Firewall settings

When setting up your firewall, you should ensure that the port settings are compatible with the HSMs and allow access to the system components you are using.

The following table identifies the ports used by the nShield system components. All listed ports are the default setting. Other ports may be defined during system configuration, according to the requirements of your organization.

| Component | Default Port | Protocol | Use |
|---|---|---|---|
| Hardserver | 9000 | TCP | Internal non-privileged connections from Java applications including KeySafe |
| Hardserver | 9001 | TCP | Internal privileged connections from Java applications including KeySafe |
| Hardserver | 9004 | TCP | Incoming impath connections from other hard servers, for example: <br><br> * From an HSM to the Remote File System (RFS). <br><br> * From a non-attended HSM to an attended host machine when using Remote Operator. |
| Hardserver in the HSM | 9004 | TCP | Incoming impath connections from client machines |
| Remote Administration Service | 9005 | TCP | Incoming connections from Remote Administration Clients |
| Audit Logging syslog | 514 | UDP | If you plan to use the Audit Logging facility with remote syslog or SIEM applications, you need to allow outgoing connections to the configured UDP port |

If you are 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 those you expect to use this port. You can also restrict the IP addresses accepted by the hardserver in the configuration file. See the *nShield Connect User Guide* for more about configuration files. Similarly if you are setting up the Remote Administration Service you need to open port 9005.

# 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 *nShield Connect User Guide* for more about creating a Security World and the appropriate Card Sets, and further configuration or setup tasks.

## 4.1. Installing the Security World Software on Windows

For information about configuring silent installations and uninstallations on Windows, see the *nShield Connect User Guide*

For a regular installation:

1. Log in as Administrator or as a user with local administrator rights.

   If the Found New Hardware Wizard appears and prompts you to install drivers, cancel this notification, and continue to install the Security World Software as normal. Drivers are installed during the installation of the Security World Software.

2. Place the Security World Software installation media in the optical disc drive.

3. Launch `setup.msi` manually when prompted.

4. Follow the onscreen instructions.

5. Accept the license terms and select **Next** to continue.

6. Specify the installation directory and select **Next** to continue.

7. Select all the components required for installation.

   By default, all components are selected. Use the drop-down menu to deselect the components that you do not want to install. **nShield Hardware Support** and **Core Tools** are necessary to install the Security World Software.

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

8. Select **Install**.

   The selected components are installed in the chosen installation directory. The installer creates links to the following nShield Cryptographic Service Provider (CSP) setup wiz-

ards as well as remote management tools under the Windows Start menu: **Start > Entrust nShield Security World**:

- If **nShield CSPs (CAPI, CNG)** was selected: **32bit CSP install wizard**, which sets up CSPs for 32-bit applications.
- If **nShield CSPs (CAPI, CNG)** was selected: **64bit CSP install wizard**, which sets up CSPs for 64-bit applications.
- If **nShield CSPs (CAPI, CNG)** was selected: **CNG configuration wizard**, which sets up the CNG providers.
- If **nShield Java** was selected: **KeySafe**, which runs the key management application.
- If **nShield Remote Administration Client Tools** was selected: **Remote Administration Client**, which runs the remote administration client.

If selected, the SNMP agent will be installed, but will not be added to the **Services** area in **Control Panel → Administrative Tools** of the target Windows machine. If you wish to install the SNMP agent as a service, please consult the *SNMP monitoring agent* section in the *nShield Connect User Guide*.

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

   The following global variables are set upon install:

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

## 4.2. Installing the Security World Software on Linux

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

1. Log in as a user with root privileges.
2. Place the installation media in the optical disc drive, and mount the drive.
3. Open a terminal window, and change to the root directory.
4. Extract the required `.tar` files to install all the software bundles by running commands of the form:

```
tar xf disc-name/linux/ver/<file>.tar.gz
```

In this command, `ver` is the architecture of the operating system (for example, i386 or amd64), and `file.tar` is the name of a `.tar.gz` file for that component.

See Software packages on the Security World software installation media 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
   ```

# 5. Before installing an HSM

## 5.1. Carefully unpack the HSM

Retain all parts of the HSM 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.

## 5.2. 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.

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

## 5.3. Check the physical security of the HSM

See the *nShield Connect and nShield 5c Physical Security Checklist*, provided in the box with the HSM.

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

# 6. Installing an HSM

This chapter describes how to install the nShield Connect in a rack, cabinet, or shelf. 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*.

> ℹ️ Always handle modules correctly. Take due account of the weight and dimensions of the nShield Connect when selecting a location for storage or installation. For more information, see *Handling an nShield Connect* in nShield Security World: nShield Connect v13.4.5 Install Guide.

> ℹ️ 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.

## 6.1. Connecting Ethernet, console 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.

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

Ensure that:

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

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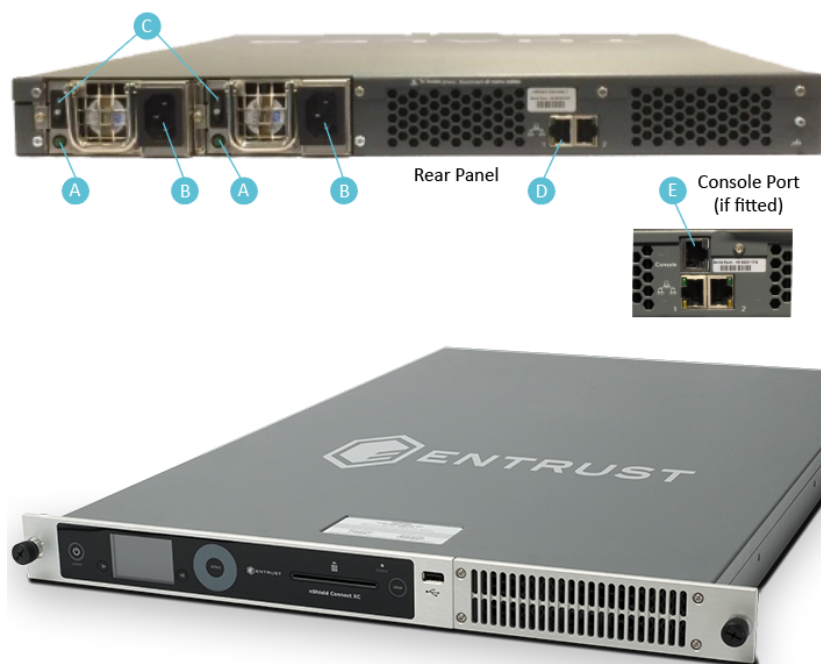
| Key | Description |
| --- | --- |
| A | Green LED if on, confirms power is on and unit is not in Standby mode |
| B | Mains power connection |
| C | Rocker switch to turn PSU on and off |
| D | Ethernet port. Two Ethernet ports are available. Port 1 is the left-hand connector when the nShield Connect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

> If you connect only one Ethernet cable to the nShield Connect, Entrust recommends that you connect it to Ethernet port 1. This is the left-hand Ethernet connector on the rear of the nShield Connect (shaded in the image).

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

For more information:

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

## 6.2. Connecting the Serial Console

On supported nShield Connect hardware variants (see *Model numbers* in nShield Security World: nShield Connect v13.4.5 Install Guide) there is a serial console port that provides access to a serial console command line interface that enables remote configuration of the nShield Connect (See the *nShield Connect User Guide*).

The RJ45 connector for the serial cable is at the rear of the nShield Connect and is labelled Console (Connecting Ethernet, console and power cables. The connector can be directly connected to your client machine or connected to a serial port aggregator for remote access. For a specification of the serial cable required, see Serial Console cable pinout information. The serial port will operate at 9600 baud, 8 data bits, no parity, and 1 stop bit (9600/8-N-1).

> ℹ️ It is recommended to use a shielded cable for the serial connection as the EMI noise from other devices in vicinity may affect the communication over the serial connection.

### 6.2.1. Serial Console cable pinout information

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

| Signal | Console Port (DTE) RJ-45 Pin | Adapter DB-9 Pin | Signal |
|--------|-------------------------------|-------------------|--------|
| CTS | 1 | 7 | RTS |
| DTR | 2 | 4 | DSR |
| TxD | 3 | 3 | RxD |
| GND | 4 | 5 | GND |
| GND | 5 | 5 | GND |
| RxD | 6 | 2 | TxD |
| DSR | 7 | 6 | DTR |
| RTS | 8 | 8 | CTS |

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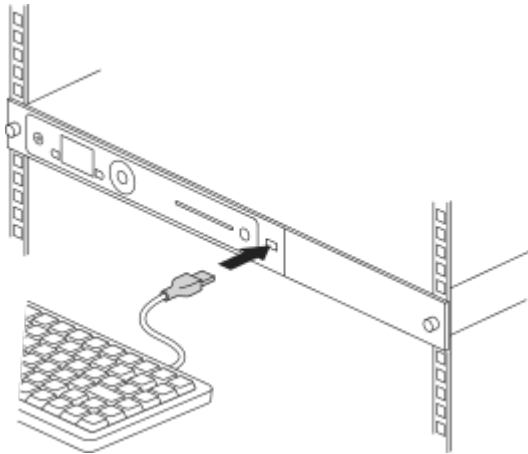
Instead of using the controls on the front panel to configure the nShield Connect, you can use a US or UK keyboard. You might find a keyboard easier for entering dates and IP addresses. You connect the keyboard to the USB connector on the front of the nShield Connect.

### 6.3.1. 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 *nShield Connect User Guide* for more about using a keyboard and keystroke shortcuts.

## 6.4. 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.

# 7. Front panel controls
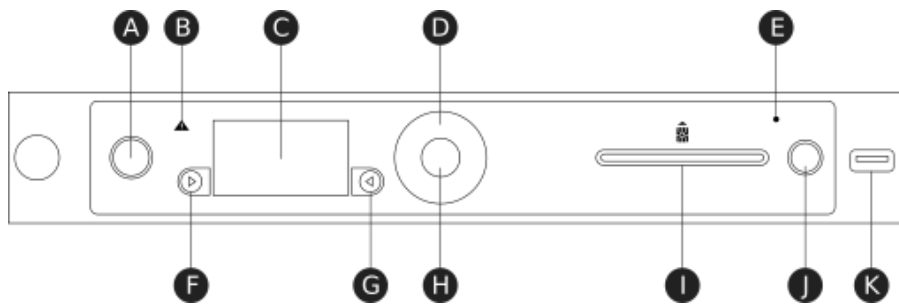


| Key | Description |
|-----|-------------|
| A | Power button |
| B | Warning LED (orange) |
| C | Display screen |
| D | Touch wheel |
| E | Status indicator LED (blue) |
| F | Display navigation button (left) |
| G | Display navigation button (right) |
| H | **Select** button |
| I | Slot for smart 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.*
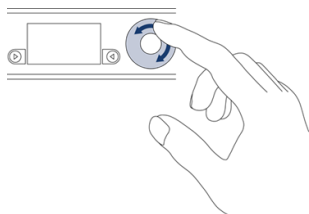


Use the touch wheel to change values or move the cursor on the display screen. To confirm a value, press the **Select** button.

# 8. Top-level menu

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.

* Submenus depend on the settings of the module.

```
1 System
    1-1 System configuration
        1-1-1 Network config
            1-1-1-1 Set up interface #1
            1-1-1-2 Set up interface #2
            1-1-1-3 Set up bond
            1-1-1-4 Set default gateway
            1-1-1-5 Set up routing *
            1-1-1-6 Show routing table
            1-1-1-7 Ping remote host
            1-1-1-8 Trace route to host
        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
            1-1-6-1 Fetch configuration
            1-1-6-2 Client config push
        1-1-7 Log config
        1-1-8 Date/time setting
        1-1-9 Keyboard layout
            1-1-9-1 UK keyboard
            1-1-9-2 US keyboard
        1-1-10 Default config
        1-1-11 Remote configuration options
            1-1-11-1 Remote mode change
    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
            1-2-6-1 View power readings
            1-2-6-2 View other readings
            1-2-6-3 Critical Errors
        1-2-7 View tamper log
        1-2-8 View unit id
    1-3 Login settings
        1-3-1 Enable UI Lockout
            1-3-1-1 UI Lockout with OCS
            1-3-1-2 UI Lockout w/out OCS
        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
2 HSM
    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
     3-1 Display World info
     3-2 Module initialization
         3-2-1 New Security World
         3-2-2 Load Security World
         3-2-3 Erase Security World
     3-3 RFS operations
         3-3-1 Update World files
         3-3-2 Remove RFS lock
     3-4 Admin operations
         3-4-1 Replace ACS
         3-4-2 Recover keys
         3-4-3 Recover PIN
         3-4-4 Set secure RTC
     3-5 Cardset operations
         3-5-1 Create OCS
         3-5-2 List cardsets
     3-6 Card operations
         3-6-1 Card details
         3-6-2 Check PIN
         3-6-3 Change PIN
         3-6-4 Erase card
     3-7 Keys
         3-7-1 List keys
         3-7-2 Verify key ACLs
     3-8 Set up remote slots *
     3-9 Set up dynamic slots
         3-9-1 Dynamic Slots
         3-9-2 Slot mapping
 4 CodeSafe *
```

# 9. Basic HSM, RFS and client configuration

> **i** The nShield nToken has been discontinued. If you already have one installed in your RFS, you can use the nToken options as described here. If you do not currently use an nToken, you must use software-based authentication.

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

- Security World Software installation and options, see Installing the software.
- The menu options, see Top-level menu.
- Advanced nShield Connect and client configuration options, see the *nShield Connect User Guide*.

> **i** An installation will have only one RFS, but may have one or more Clients. The RFS can also dual role as a Client. Before you can continue with the following configuration, the RFS and every Client must have the Security World software installed, see Installing the software.

## 9.1. About nShield Connect and client configuration

An nShield Connect and a client communicate using their hardservers. These handle secure transactions between the HSM and 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.

> **i** Multiple nShield HSMs can be configured to communicate with one client, just as multiple clients can be configured to communicate with one nShield Connect.

### 9.1.1. Remote file system (RFS)

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

## 9.1.2. HSM 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 *nShield Connect User Guide* for more about nShield Connect configuration files and advanced configuration options.

## 9.1.3. Client configuration

The current configuration files for the hardserver of a client are stored in its local file system.

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

> The following steps assume that you have added the path `%NFAST_HOME%\bin` (Windows) or `/opt/nfast/bin/` (Linux) to the `PATH` system variable.

# 9.2. 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 *nShield Connect User Guide* for more about creating a Security World and the OCS.

## 9.2.1. Configuring the Ethernet interfaces - IPv4 and IPv6

An nShield Connect communicates with one or more clients over an Ethernet network. You must supply IP addresses for the nShield Connect and the client. Contact your system

administrator for this information if necessary.

There are two network interfaces on the nShield Connect. Three configurations are supported:

- Single network interface.
- Two independent network interfaces.

  You must connect the interfaces to physically different networks.

- The two network interfaces combined as a bond interface.

  The bond interface can use:

  - Active backup mode.
  - 802.3ad mode (requires a switch that supports 802.3ad).

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 following can be configured:

- Interface addresses
- Bond
- 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.

> 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 *nShield Connect User Guide* for more information.

### 9.2.1.1. IPv4 and IPv6

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

- IPv4 only

- IPv4 and IPv6
- IPv6 only.

> ℹ Interface#1 is enabled by default and cannot be disabled. Interface #2 is disabled by default and can be enabled and disabled.

### 9.2.1.1.1. 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.

### 9.2.1.1.2. 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:

- The long representation is x:x:x:x:x:x:x:x, where each x is a field containing 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`

- 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`

  `::` can only appear once in an IPv6 address.

Unless the address is a link-local address, the nShield Connect front panel only allows

lower-case letters 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.

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.

### 9.2.1.1.3. IPv6 compliance

A new sub-menu (1-1-1-9 - **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.

### 9.2.1.1.4. 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 Valid IPv6 Addresses.

| Use Case | Acceptable Address Type |
| --- | --- |
| Static IPv6 Address Entry | • Global Unicast<br>• Local Unicast |

| Use Case | Acceptable Address Type |
|---|---|
| IPv6 Default Gateway | • Global Unicast<br>• Local Unicast<br>• Link-local |
| IPv6 Route Entry - IP Range | • Unknown<br>• Loopback<br>• Global Unicast<br>• Local Unicast<br>• Link local<br>• Teredo<br>• Benchmarking<br>• Orchid<br>• 6to4<br>• Documentation<br>• Multicast |
| IPv6 Route Entry - Gateway | • Global Unicast<br>• Local Unicast<br>• Link-local |
| RFS Address | • Global Unicast<br>• Local Unicast |
| Client Address | • Global Unicast<br>• Local Unicast |
| Push Client Address | • Global Unicast<br>• Local Unicast |
| Ping | • Unknown<br>• Loopback<br>• Global Unicast<br>• Local Unicast<br>• Link-local<br>• Teredo<br>• Benchmarking<br>• Orchid<br>• 6to4<br>• Documentation<br>• Multicast |

| Use Case | Acceptable Address Type |
|---|---|
| Traceroute | • Unknown<br>• Loopback<br>• Global Unicast<br>• Local Unicast<br>• Link-local<br>• Teredo<br>• Benchmarking<br>• Orchid<br>• 6to4<br>• Documentation<br>• Multicast |

### 9.2.1.2. 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 net work 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 appropri- ate configuration item and pushing an nShield Connect configuration file.

## 9.2.2. Configure Ethernet interface #1

To set up Ethernet interface #1 (default):

### 9.2.2.1. 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:

   ```
   Network configuration

   IPv4 enable/disable:
   ```

---

```
ENABLE

CANCEL    FINISH
```

2. Set the **ENABLE/DISABLE** field to the required option.

3. To accept, press the right-hand navigation button.

### 9.2.2.2. 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:
       0.  0.  0.  0
   Enter netmask:
       0.  0.  0.  0
   CANCEL          NEXT
   ```

2. Set each field of the IP address and netmask for the interface (press the **Select** button to move to the next field).

3. Once all fields have been set, press the right-hand navigation button to continue.

4. To accept the changes, press the right-hand navigation button and then **CONTINUE** to go back to the **Static IPv4 address** menu.

### 9.2.2.3. 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 > Enable/Disable IPv6**.

   The following screen displays:

   ```
   Network configuration

   IPv6 enable/disable:
   DISABLE

   CANCEL    FINISH
   ```

2. Set the **ENABLE/DISABLE** field to the required option.

3. To accept, press the right-hand navigation button.

### 9.2.2.4. 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 addr/SLAAC > Select Static/SLAAC**.

   The following screen is displayed:

   ```
   Network configuration
   Do you want to use a
   static address or
   SLAAC?
   ```

   Select static and press the right-hand navigation button.

   Then, select **Static IPv6 address** and press the right-hand navigation button.

   The following screen displays:

   ```
   Network configuration
   Enter IPv6 address
   For interface #1:



   CANCEL    NEXT
   ```

2. Enter the required IPv6 address.

3. 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
   ```

4. When the IPv6 address prefix details are correct, press the right-hand navigation button.
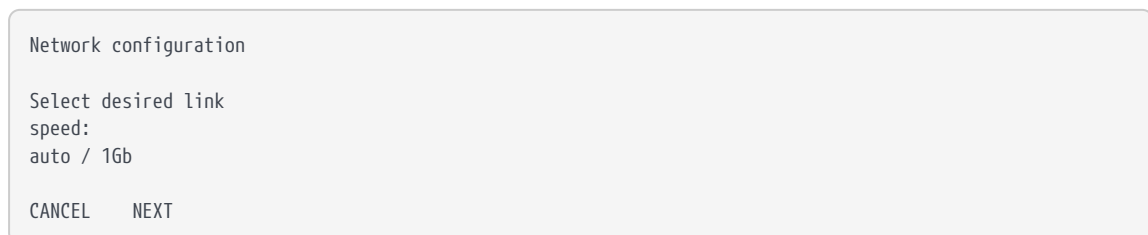
5. You are asked whether you wish to accept the new interface. To accept, press the right-hand navigation button.

Enabling static IPv6 addresses on HSM's network interface disables SLAAC on this interface. See Enable IPv6 SLAAC for SLAAC addresses.

### 9.2.2.5. 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**.

> 🛈 Entrust recommends 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.

3. 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.
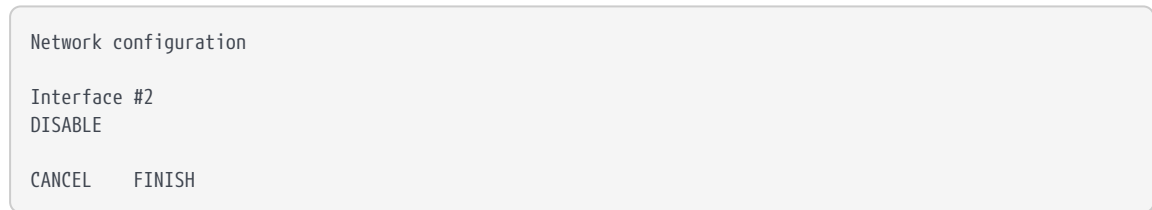
## 9.2.3. Configure Ethernet interface #2

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
```

5. Select the **ENABLE** option.
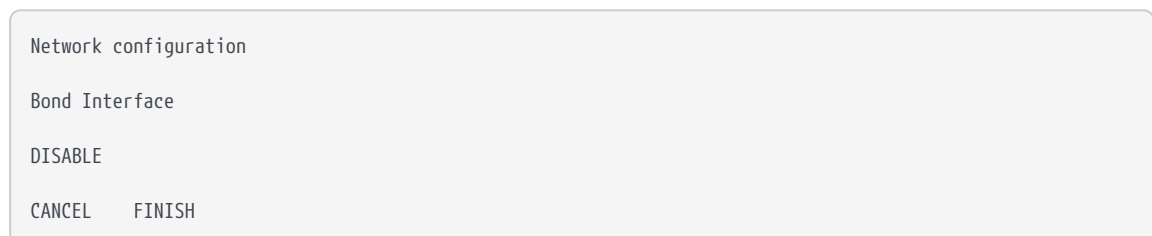
6. Press the right-hand navigation button to accept. A screen similar to that used for inter face #1 is displayed.

## 9.2.4. Configure an Ethernet bond interface

### 9.2.4.1. Enable or disable the use of a bond interface

1. From the front panel menu, select **System > System configuration > Network config > Set up bond > Enable/disable bond**.

   The following screen displays:

```
Network configuration

Bond Interface

DISABLE

CANCEL    FINISH
```
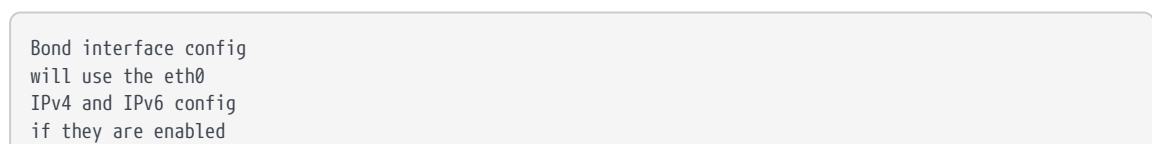
2. Set the **ENABLE/DISABLE** field to the required option.

3. To accept, press the right-hand navigation button.

### 9.2.4.2. Set up a bond interface

1. From the front panel menu, select **System > System configuration > Network config > Set up bond > Configure bond**.

   The following screen displays:

```
Bond interface config
will use the eth0
IPv4 and IPv6 config
if they are enabled
```

```
CANCEL   NEXT
```

2. Press the right-hand navigation button.

   The following screen displays:

   ```
   Bond interface config
   Update parameter

   mode: 802.3ad

   BACK    NEXT
   ```

3. Set the mode field to the required option, either `802.3ad` or `active-backup`.

4. To accept, press the right-hand navigation button.

   The following screen displays:

   ```
   Bond interface config
   Update parameter

   miimon: 100

   BACK    NEXT
   ```

5. Set the `miimon` field to the required value, the range is `0 - 10000` milliseconds.

   Setting the `miimon` value to `0` disables it. This can prevent the bonding resilience from functioning correctly in `active-backup` mode.

6. To accept, press the right-hand navigation button.

   The following screen displays:

   ```
   Bond interface config
   Update parameter

   lacp_rate: slow

   only valid for
   802.3ad (LACP) mode

   BACK    NEXT
   ```

7. Set the `lacp_rate` field to the required option, either `slow` or `fast`.

   This parameter is only valid for 802.3ad mode. This setting is ignored in other modes.

   **slow**      request LACPDUs to be transmitted every 30 seconds

> **fast**      request LACPDUs to be transmitted every 1 second

8. To accept, press the right-hand navigation button.

   The following screen displays:

   ```
   Bond interface config
   Update parameter
   xmit hash policy:
   layer2

   only valid for
   802.3ad (LACP) mode

   BACK     NEXT
   ```

9. Set the `xmit hash policy` field to the required option.

   This parameter is only valid for 802.3ad mode. This setting is ignored in other modes.

   Options:

   ◦ layer2

   ◦ encap2+3

   ◦ layer2+3.

   For more information, see https://www.kernel.org/doc/Documentation/networking/bonding.txt

10. To accept, press the right-hand navigation button.

    The following screen displays:

    ```
    Bond interface config
    Update parameter

    primary device: eth0

    only valid for
    active-backup mode

    BACK     NEXT
    ```

11. Set the `primary device` field to the required option, either `eth0` or `eth1`.

    This parameter is only valid for `active backup` mode. This setting is ignored in other modes.

12. To accept, press the right-hand navigation button.

    The following screen displays:

```
Bond interface config
Update parameter

resend igmp: 1

only valid for
active-backup mode

BACK    NEXT
```

13. Set the `resend igmp` field to the required value. Range: `0` - `255`.

    This parameter is only valid for `active backup` mode. This setting is ignored in other modes.

14. To accept, press the right-hand navigation button.

    The following screen displays:

```
Bond interface config

Are you sure you wish
to change the config ?

CANCEL    CONFIRM
```

15. To accept and apply changes to the bond config, press the right-hand navigation button.

    The following confirmation screen displays:

```
Bond interface
config completed OK

CONFIRM
```

## 9.2.5. Default gateway

### 9.2.5.1. 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
```

2. Enter the IPv4 address of the default gateway.

3. Press the right-hand navigation button **NEXT** and then **FINISH** to accept.

### 9.2.5.2. 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:

::

CANCEL    NEXT
```

   Select the interface for the IPv6 gateway. Press the right-hand navigation button to accept.
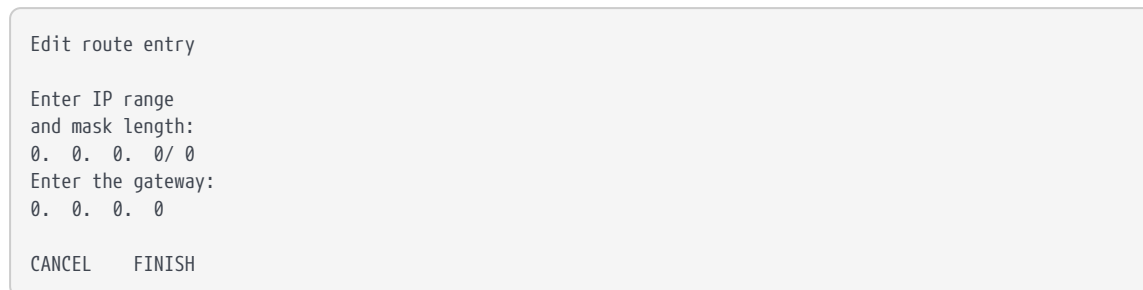
## 9.2.6. Set up Routing

### 9.2.6.1. Set up routing for IPv4

To set a new route entry for IPv4:

1. 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
   ```
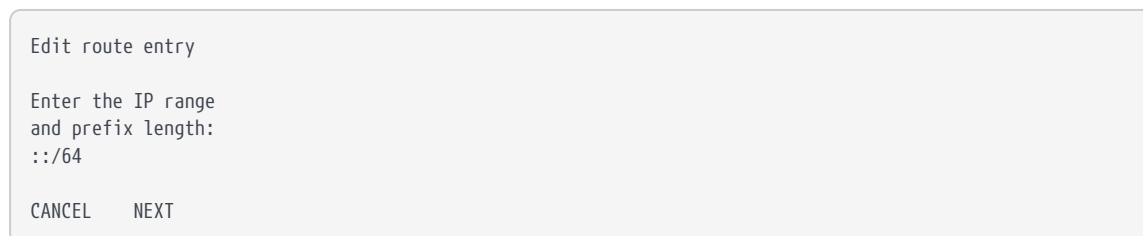
2. Enter the IPv4 address range details for the route. Press the right-hand navigation button to accept.

## 9.2.6.2. Set up routing for IPv6

To set a new route entry for IPv6:

1. 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
   ```

2. 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
   ```

3. 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
```

4. Select the interface for the IPv6 gateway and press the right-hand navigation button to accept.

5. 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.

## 9.2.7. Edit route entry

### 9.2.7.1. 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
```

2. 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
```

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

## 9.2.7.2. Edit IPv6 route entry

To edit a route entry for IPv6:

1. 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
   ```

2. 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
   ```

3. 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
   ```

4. 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
   ```

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

## 9.2.8. 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**.
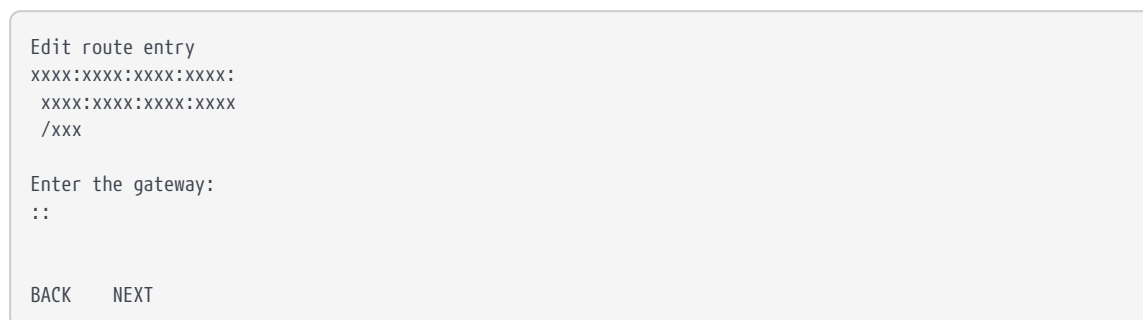
   The following screen is displayed:

   ```
   ►  1. 1. 1. 1/ 1
   3. 3. 3. 3/ 3
   1111:1111:1111:1111:
   1111:1111:1111:1111
   /128


   BACK    SELECT
   ```
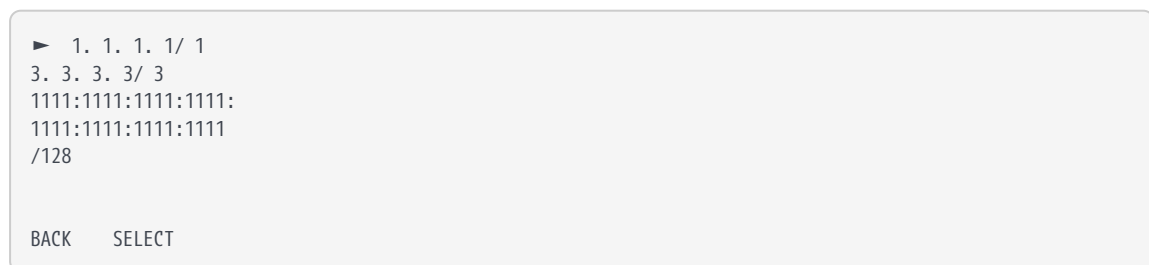
2. Select the IPv4/IPv6 route to be removed. Press the right-hand navigation button.

3. The selected route will be displayed. Press the right-hand navigation button to remove the route.

## 9.2.9. 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 > Static addr/SLAAC > Select Static/SLAAC**.

   The following screen is displayed:

   ```
   Network configuration
   Do you want to use a
   static address or
   SLAAC?
   ```
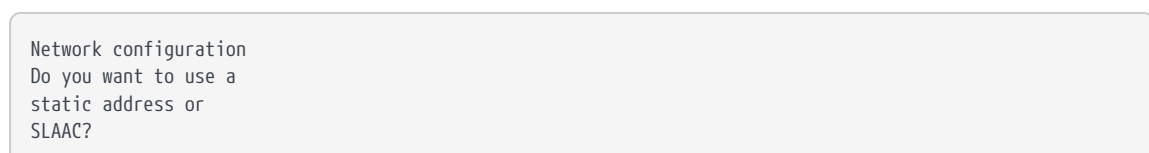
2. Select **SLAAC** and press the right-hand navigation button.

3. The **IPv6 address config selected** screen is displayed. Press the right-hand navigation button to accept.

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.

> ℹ️ Enabling SLAAC on the HSM's network interface disables the use of static IPv6 addresses on this interface.

## 9.2.10. Configuring the Remote File System (RFS)

The RFS contains the master copy of the Security World data for backup purposes. The RFS can be a standalone machine, and can also dual role as a client. If the RFS duals as a client, a common file structure serves both the RFS and the configuration files for the client.

See the *nShield Connect 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, or both.

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 $K_{NETI}$ key ($HK_{NETI}$). The $K_{NETI}$ 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 $K_{NETI}$ key by giving the following command on the client computer. For guidance on network security, see the *nShield Security Manual*.

```
anonkneti <Unit IP>
```

In this command, *<Unit IP>* is the IP address of the nShield Connect, which could be one of the following:

- an IPv4 address
- an IPv6 address, including a link-local IPv6 address

- a hostname

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 $K_{NETI}$ 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 and nShield Connect in the following order:

1. Prepare the RFS by running the following command on that computer:

```
rfs-setup <Unit IP> A285-4F5A-7500 2418ec85c86027eb2d5959fef35edc5e1b3b698f
```

   In this command:

   - *<Unit IP>* is the IP address of the nShield Connect.
   - `A285-4F5A-7500` is the ESN of the nShield Connect.
   - `keyhash` is the hash of the $K_{NETI}$ key.

2. On the nShield Connect display screen, use the right-hand navigation button to select **System > System configuration > Remote file system**, and enter the IP address of the client computer on which you set up the RFS:

```
   Remote File System

Enter IP address:



CANCEL        CONTINUE
```

3. The next screen asks for the port number on which the RFS is listening. Enter the port number and press the right-hand navigation button to continue:

```
   Remote File System

Enter port number:
    9004

CANCEL        CONTINUE
```

ℹ️ | Leave the port number at the default setting of 9004.

4. Select the config push mode and press the right-hand navigation button to continue:

```
   Remote File System

Set RFS config push
mode to:

        AUTO

CANCEL        CONTINUE
```

Three options are available:

- AUTO: The RFS is only allowed to push configuration files to the nShield Connect if secure authentication is enabled. This is the default value.
- ON: The RFS is allowed to push configuration files to the nShield Connect.
- OFF: The RFS is not allowed to push configuration files to the nShield Connect.

5. You must then choose whether to enable or disable secure authentication when setting up the RFS. The following screen is displayed:

```
   Remote File System

Do you want secure
authentication enabled
on the RFS?

        YES
CANCEL        CONTINUE
```

a. Select No and press the right-hand navigation button to configure the RFS without secure authentication. The authentication of the RFS will be based on the IP address only.

b. Select Yes and press the right-hand navigation button to configure the RFS with secure authentication.

6. Skip this step if you have not selected secure authentication.

If an nToken is installed in the RFS, you will be asked to choose which authentication key to use. Select the desired option and press the right-hand navigation button:

```
>0DA8-A5AE-BA0D
 Software Key


BACK      SELECT
```

> a. The ESN of the nToken installed in the RFS.
>
> b. "Software Key" for software-based authentication.

If no nToken is installed in the RFS, then software-based authentication is automatically selected.

7. Skip this step if you have not selected secure authentication.

    The next screen will ask you to verify that the key hash displayed by the nShield Connect matches the RFS key hash:

    ```
    Remote 0DA8-A5AE-BA0D
    reported the key hash:
     9e0020264af732933574
     0cfe10446d33cea33f4a
    Is this EXACTLY right?

    CANCEL        CONFIRM
    ```

    The RFS key hash is obtained by running the commands described below. Take a copy of the returned key hash and compare it to the value reported on the nShield Connect display.

    **With software-based authentication**

    Run the following command on the RFS:

    ```
    enquiry -m0
    ```

    This command returns the software key hash, tagged as `kneti hash`, as part of its output, for example:

    ```
    Server:
      enquiry reply flags   none
      enquiry reply level   Six
      ...
      kneti hash            d4c3d757a67416cb9ba31f33febd6ead688629e5
      ...
    ```

    **With nToken authentication**

    Run the following command on the RFS:

    ```
    ntokenenroll -H
    ```

    This command produces output of the form:

    ```
    nToken module #1
    nToken ESN:     0DA8-A5AE-BA0D
    ```

```
nToken key hash: 9e0020264af732933574
                 0cfe10446d33cea33f4a
```

Check that the ESN also matches the one reported on the nShield Connect display.

If the RFS key hash matches the one reported on the nShield Connect display, press the right-hand navigation button to continue the RFS configuration. Otherwise press the left-hand navigation button to cancel the operation.

8. The nShield Connect displays "Transferring files..." followed by a message reporting that the RFS has been set up. Press the right-hand navigation button again to exit.

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

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

### 9.2.10.1. Systems configured for Remote Administration

Before using Remote Administration or configuring NTP, enable *config push* on the nShield Connect for the RFS or client computer you intend to use for configuration. The RFS config push is preferred unless the config push client is not actually the same machine as the RFS. The RFS config push is recommended at least when securely bootstrapping the configuration of the system from the nShield Connect front panel.

## 9.2.11. Enabling config push from the RFS

On the nShield Connect display, use the right-hand navigation button to select **System > System configuration > Remote File System**, and follow the steps described in Configuring the Remote File System (RFS). To enable config push from the RFS, set the push mode to **AUTO** with RFS secure authentication enabled (recommended), or to **ON**.

> The RFS config push supports specifying secure authentication from the nShield Connect front panel, whereas the client config push only supports specifying authentication either from the nShield Connect Serial Console push command, or from the config file itself.

## 9.2.12. Enabling config push from a client computer

To enable config push from a client computer, on the nShield Connect display, use the right-hand navigation button to select **System > System configuration > Config file**

**options > Client config push > Config push mode**, set **ON** or **OFF**, then select **CONFIRM**. A confirmation message will be displayed.

After enabling config push, specify the IP address of the client to push the configuration from. On the nShield Connect display, use the right-hand navigation button to select **System > System configuration > Config file options > Client config push > Client address**. Enter the IP address and select **CONFIRM**. A message is displayed confirming your chosen IP address. Select **CONTINUE**.

> ⊗ Any remote computer is allowed to push configuration files if no IP address or the 0.0.0.0 address is specified.

After enabling config push, complete the configuration steps by editing the configuration files, rather than by using nShield Connect front panel. See the *nShield Connect User Guide* for more about configuration files.

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

### 9.3.1. Client configuration utilities

Entrust provides the following utilities for client configuration:

| Utility | Description |
|---------|-------------|
| `nethsmenroll` | Used to configure the client to communicate with the nShield Connect. |
| `config-serverstartup` | Used to configure the hardserver of the client to enable TCP sockets. |

#### 9.3.1.1. nethsmenroll

The `nethsmenroll` command-line utility edits the client hardserver's configuration file to add the specified nShield Connect. If the nShield Connect's `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 <hsm-ip> <hsm-esn> <hsm-kneti-hash>
```

*Options*:

| | |
|---|---|
| `-m\|--module=MODULE` | Specifies the local module number that should be used (default is `0` for dynamic configuration by hardserver). |
| `-p\|--privileged` | Makes the hardserver request a privileged connection to the nShield Connect (default `unprivileged`). |
| `-<hsm-ip>` | The IP address of the nShield Connect, which could be one of the following:<br><br>• an IPv4 address<br>• an IPv6 address, including a link-local IPv6 address<br>• a hostname |
| `-r\|--remove` | Removes the configuration of the specified nShield Connect. |
| `-f\|--force` | Forces reconfiguration of an nShield Connect already known. |
| `--no-hkneti-confirmation` | Does not request confirmation when automatically determining the nShield Connect's `ESN` and `HKNETI`.<br><br>⚠ 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. For guidance on network security, see the *nShield Security Manual*. |
| `-V\|--verify-nethsm-details` | When the `ESN` and `HKNETI` have been provided on the command line, verifies that the selected HSM is online, reachable and matches those details. |
| `-P\|--port=PORT` | Specifies the port to use when connecting to the given nShield Connect (default `9004`). |
| `-n\|--ntoken-esn=ESN` | Specifies the `ESN` of the nToken to be used to authenticate this client. If the option is omitted, then software authentication will be used instead. |

### 9.3.1.2. 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
```

## 9.3.2. 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.

> **ⓘ** 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.

## 9.3.3. 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 HSM, RFS and client configuration for more about the available options.

Do the following:

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

   ```
   nethsmenroll --help
   ```

2. 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.

3. Do one of the following:

   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>
   ```

   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.
   ```

### 9.3.4. Configure the TCP sockets on the client for Java applications

To configure the TCP sockets on the client for Java applications (for example, KeySafe):

1. Run the command:

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

## 9.4. 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 client**.

   The following screen is displayed:

   ```
   Client configuration

   Please enter your
   client IP address:



   CANCEL          NEXT
   ```

   Enter the IP address of the client, and press the right-hand navigation button.

2. Use the touch wheel to confirm whether you want to save the IP or not, and press the right-hand navigation button.

```
Client configuration

Do you want to save
the IP in the config?
(No for dynamic client
IPs)
          No
BACK            NEXT
```

3. Use the touch wheel to select the connection type between the nShield Connect and the client.

```
Client configuration

Please choose the
client permissions

    Unprivileged

BACK            NEXT
```

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 Linux. |
| Priv. on any ports | Privileged connections are allowed on all ports. |

> ℹ️ 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. Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

4. When you have selected a connection option, press the right-hand navigation button.

The following screen is displayed:

```
Client configuration
```

```
Do you want secure
authentication enabled
on this client?

        Yes
BACK            NEXT
```

    a. Select No and press the right-hand navigation button to configure the client with-
       out secure authentication. The authentication of the client will be based on the IP
       address only.

    b. Select Yes and press the right-hand navigation button to configure the client with
       secure authentication.

5. On the nShield Connect, enter the number of the port on which the client is listening
   (the default is 9004), and press the right-hand navigation button. The following screen
   is displayed:

```
Client configuration

On what port is the
client listening?

        9004

CANCEL          NEXT
```

6. Skip this step if you have not selected secure authentication.

   If an nToken is installed in the client, you will be asked to choose which authentication
   key to use. Select the desired option and press the right-hand navigation button:

```
>3138-147F-2D64
 Software Key


BACK      SELECT
```

    a. The ESN of the nToken installed in the client.
    b. "Software Key" for software-based authentication.

   If no nToken is installed in the client, then software-based authentication is automati-
   cally selected.

> Software-based authentication is only supported from version
> 12.60.

7. Skip this step if you have not selected secure authentication.

   The next screen will ask you to verify that the key hash displayed by the nShield Con-

nect matches the client key hash:

```
Remote 3138-147F-2D64
reported the key hash:
 691be427bb125f387686
 38a18bfd2eab75623320
Is this EXACTLY right?

CANCEL        CONFIRM
```

The client key hash is obtained by running the commands described below. Take a copy of the returned key hash and compare it to the value reported on the nShield Connect display.

**With software-based authentication**

Run the following command on the client:

```
enquiry -m0
```

This command returns the software key hash, tagged as `kneti hash`, as part of its output, for example:

```
Server:
  enquiry reply flags    none
  enquiry reply level    Six
  ...
  kneti hash             f8222fc007be38b78ebf442697e244dabded38a8
  ...
```

**With nToken authentication**

Run the following command on the client:

```
ntokenenroll -H
```

This command produces output of the form:

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

Check that the ESN also matches the one reported on the nShield Connect display.

If the client key hash matches the one reported on the nShield Connect display, press the right-hand navigation button to continue the RFS configuration. Otherwise press the left-hand navigation button to cancel the operation.

8. The nShield Connect displays a message reporting that the client has been configured. Press the right-hand navigation button again.

See the *nShield Connect User Guide* for more about modifying or deleting an existing client, configuring multiple clients, client licenses, pushing configuration files to the nShield Connect, and advanced configuration options.

## 9.5. Restarting the hardserver

In order to establish any configuration changes you may have entered, you must restart the hardserver (also called the nfast server).

1. 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"
   ```

   b. **Linux**:

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

## 9.6. Zero touch configuration of an nShield Connect

On a serial-enabled nShield Connect (see *Model numbers* in nShield Security World: nShield Connect v13.4.5 Install Guide) you can configure the nShield Connect and set up the RFS by using the nShield Connect Serial Console rather than the front panel. See the *nShield Connect User Guide* for more information on the Serial Console.

Once the nShield Connect's power, Ethernet and serial cables have been connected, to allow zero touch configuration of the nShield Connect (no further use of the front panel required), follow these steps:

### 9.6.1. Configuring the network interfaces via the Serial Console

1. Log in to the nShield Connect Serial Console (see the *nShield Connect User Guide*).
2. Configure networking on Ethernet Interface #1:
   a. Set the IP address and netmask of the interface:

```
(cli) netcfg iface=0 addr=0.0.0.0 netmask=0.0.0.0
```

b. Set the IP address of the gateway for the nShield Connect:

```
(cli) gateway 0.0.0.0
```

If your network environment requires you to configure static routes you may also use the nShield Connect Serial Console to configure static routes for the nShield Connect at this stage.

## 9.6.2. Allowing configuration files to be pushed to the nShield Connect via the Serial Console

To allow the Remote File System (RFS) to push configuration files to the nShield Connect, configure the RFS using the `rfsaddr` command. To allow other remote computers to push configuration files to the nShield Connect, use the `push` command.

### 9.6.2.1. Configuring the Remote File System (RFS) via the Serial Console

1. Log in to the nShield Connect Serial Console (see *Creating a serial console session* in the *nShield Connect User Guide*), and run the following commands to obtain the nShield Connect ESN and KNETI hash, for example:

```
(cli) esn
ESN: 6B1D-03CE-2F9A
(cli) kneti
Kneti hash: 56304e3f752cd13d219fa47ad27d56bb6a6642aa
```

2. Run the `rfs-setup` command on the RFS with the IP address of the nShield Connect and the values previously returned by the `esn` and `kneti` commands:

```
rfs-setup <Unit IP address> <ESN> <KNETI hash>
```

For information on running `rfs-setup`, see Configuring the Remote File System (RFS).

3. In the nShield Connect Serial Console, configure the RFS using the `rfsaddr` command.

```
(cli) rfsaddr address[:port] [keyhash [esn]] [push]
```

In this command:

- ◦ `address` is the RFS IP address.
- ◦ `port` is the RFS port number (default is 9004).
- ◦ `keyhash` is the RFS KNETI hash (default is 40 zeroes).
- ◦ `esn` is the RFS nToken ESN (default is "", i.e. no ESN).
- ◦ `push` specifies if the RFS can push configuration files to the nShield Connect:
  - ▪ `ON`: The RFS is allowed to push configuration files.
  - ▪ `OFF`: The RFS is not allowed to push configuration files.
  - ▪ `AUTO`: The RFS is allowed to push configuration files if RFS secure authentication is enabled. This is the default option.

The `keyhash` and `esn` are optional, and can be used to enable the RFS secure authentication:

a. No RFS secure authentication (not recommended): The `keyhash` and `esn` parameters are not specified.

b. RFS software-based authentication: Only the `keyhash` parameter is specified. The RFS software KNETI hash is obtained by running the `enquiry -m0` command on the RFS. The value is tagged as `kneti hash` in the command output.

c. RFS nToken authentication: The `keyhash` and `esn` parameters are specified. The RFS nToken KNETI hash and ESN are obtained by running the `ntokenenroll -H` command on the RFS.

### 9.6.2.2. Allowing configuration files to be pushed to the nShield Connect from a remote computer via the Serial Console

In addition to the RFS, the `push` serial command can be used to allow a remote computer to push configuration files.

```
(cli) push ON [address] [keyhash]
```

In this command:

- `address` is the remote computer IP address. It defaults to 0.0.0.0 which allows any address to push. It is not recommended to leave the IP address unrestricted, unless `key hash` is specified for authentication.
- `keyhash` is the hash of the key with which the authorized client is to authenticate itself (defaults to no key authentication required).

> **!** Enabling the push feature allows remote computers to change the HSM configuration file and make configuration changes that are normally only available through the HSM secure user interface.

After you enable the nShield Connect for zero touch configuration, everything that can be configured using the front panel can be configured remotely using one of the following methods:

- The nShield Connect Serial Console.
- The `cfg-pushnethsm` utility to push an updated configuration file to the nShield Connect (see the *nShield Connect User Guide*). From the configuration file you can configure the RFS, add clients, or change the network configuration.
- The `nethsmadmin` utility (see the *nShield Connect User Guide*).

## 9.7. 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
```

For an example of the output following a successful `enquiry` command. See Enquiry utility.

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.

## 9.8. Using a Security World

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

# 10. Troubleshooting

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

## 10.1. Checking operational status

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

### 10.1.1. 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 Linux.

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

```
 Server:
  enquiry reply flags  none
  enquiry reply level  Six
  serial number        ####-####-####
  mode                 operational
  version              #-#-#
  speed index          ######
  rec. queue           ####..####
  ...
  version serial       #
  remote port (IPv4)   ####

 Module ##:
  enquiry reply flags  none
  enquiry reply level  Six
  serial number        ####-####-####
  mode                 operational
  version              #-#-#
  speed index          #####
  rec. queue           ##..###
  ...
  rec. LongJobs queue  ##
  SEE machine type     PowerPCELF
  supported KML types  DSAp1024s160 DSAp3072s256
  hardware status      OK
```

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.

### 10.1.2. Status LED

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

| Status LED | Description |
|---|---|
| Off. | **Status: Power off or Standby mode**<br><br>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.<br><br>If you believe the module's power supply unit has failed, contact Support. |
| On, occasionally blinks off. | **Status: Operational mode**<br><br>The module is in Operational mode and accepting commands. The more frequently the Status LED blinks off, the greater the load on the module. |
| Flashes two short pulses, followed by a short pause. | **Status: Initialization mode**<br><br>Existing Security World data on the module has been erased.<br><br>The module is automatically placed in Initialization mode after a Security World is created. For more information, see the *nShield Connect User Guide*. |
| Flashes two long pulses followed by a pause. | **Status: Maintenance mode**<br><br>Used for reprogramming the module with new firmware.<br><br>The module only goes into Maintenance mode during a software upgrade. |
| Flashes SOS, the Morse code distress code (three short pulses, three long pulses, three short pulses).<br><br>After flashing SOS, the Status LED flashes a Morse code letter which identifies the error. | **Status: Error mode**<br><br>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.<br><br>For internal security modules running firmware 2.6.1.2 and above, the error code is also reported by the `enquiry` utility in the `hardware status field` of the `Module` and under `hardware errors` in the hardserver log.<br><br>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.<br><br>For information about error codes, see the *nShield Connect User Guide*. |

### 10.1.3. 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) 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*.

### 10.1.4. Orange warning LED

If the orange warning LED 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**.

### 10.1.5. 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*.

### 10.1.6. 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. |

| Footer color | Text in footer | Meaning |
|---|---|---|
| Red | HSM Failed | The internal module has failed. See Orange warning LED for more information. |

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

> ℹ️ The blue Status LED flashes to indicate the status of the internal security module.

## 10.1.7. Power button

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

> ℹ️ 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. |

## 10.1.8. 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. |

# 10.2. Module overheating

If the internal module of the HSM exceeds the safe operating temperature, the unit stops operating and displays the SOS-T error message on the Status LED. See Status LED for details of the SOS-T error message.

# 10.3. 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.

## 10.3.1. Information

This type of message indicates routine events:

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

```
nFast Server service stopping
```

## 10.3.2. Notice

This type of message is sent for information only:

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

## 10.3.3. Client

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

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

## 10.3.4. Serious error

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

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

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

## 10.3.5. Serious internal error

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

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

If you receive a serious internal error, contact Support.

## 10.3.6. Start-up errors

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

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

Reinstall the Security World software, see Installing the software. If reinstallation does not solve the problem, contact Support.

### 10.3.7. Fatal errors

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

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

or

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

If you receive either of these errors, contact Support.

## 10.4. Utility error messages

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

### 10.4.1. 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 no power is supplied to the nShield Connect unit.

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 this case is to leave the nShield Connect powered up for at least 10 hours to recharge the battery, and then reset the clock. No other nonvolatile data is lost when this occurs.

# 11. HSM 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 validations for the HSM, 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 allow a fan tray to be removed from the nShield Connect for longer 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.

## 11.1. 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.

# 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 *nShield Connect and nShield 5c Slide Rails Instructions*. |
| USB keyboard | M-030099-L | For more information about using a USB keyboard with the HSM, see Connecting the optional USB keyboard. |
| 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.

# 13. Uninstalling existing software

Entrust recommends that you uninstall any existing older versions of Security World Software before you install new software. In Windows environments, if the installer detects an existing Security World Software installation, it asks you if you want to install the new components. These components replace your existing installation.

The automated Security World software installers do not delete user created components, key data, or Security World data. However, on Linux, a manual installation using `.tar` files *does* overwrite existing data and directories.

> Before you uninstall the Security World Software, Entrust strongly recommends that you make a secure backup of any existing Security World and nShield configuration files. See the *nShield Connect User Guide* for more information.

> When upgrading the Security World Software, you do not need to delete key data or any existing Security World. If you want to do so for other reasons, see the *nShield Connect User Guide* for more information. If you do delete Security World data, it cannot be restored unless you have an up-to-date backup and a quorum of the Administrator Card Set (ACS) is available.

> The file `nCipherKM.jar`, if present, is located in the extensions folder of your local Java Virtual Machine. The uninstall process may not delete this file. Before reinstalling over an old installation, remove the `nCipherKM.jar` file. See the *nShield Connect User Guide* for more about locating the Java Virtual Machine extensions folder.

> In Windows environments, because the hardserver is installed as a named service (known as the nFast server), it is only possible to have one Security World Software installation on any given computer. It is also not possible to have more than one Security World Software installation on the same computer on Linux.

> If you are downgrading a software authenticated client to a Security World Software earlier than version 12.60, the client will need to be re-enrolled as software-based authentication is not supported. See the *nShield Connect User Guide*, section "Configuring the nShield Connect to use the client", for more information.

> ⊗ Entrust recommends that you do not uninstall the Security World Software unless you are either certain it is no longer required, or you intend to upgrade it.

## 13.1. Uninstalling the Security World Software on Windows

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

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

## 13.2. Uninstalling the Security World Software on Linux

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

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

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

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

```
$ su -
```

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

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

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

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

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

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

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

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

   a. `userdel -r nfast` and `userdel -r ncsnmpd` will remove the users.

   b. `groupdel nfast` and `groupdel ncsnmpd` will remove the groups.

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

# 14. Software packages on the Security World software installation media

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

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

## 14.1. Security World installation media

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

### 14.1.1. Component bundles

| Linux Package | Windows Feature in the Installer | Content |
|---|---|---|
| hwsp | nShield Hardware Support | Hardware Support package, including the nShield Server and device driver. |
| ctls | nShield Core Tools | Management utilities, including generatekey, diagnostic and performance tools, Remote Administration Client tools, and the PKCS#11 library. |
| ctd | nShield Cipher Tools | Developer package example programs, and developer libraries for the nCore API and generic stub. |
| devref | nShield Developer Reference | Reference Documentation for the nCore API. |
| N/A | nShield CSPs (CAPI, CNG) | CAPI and CNG providers and associated tools. |
| N/A | nShield Debug | PDB and .map files for nShield libraries and executables. |
| N/A | nShield Device Drivers | Device drivers for PCI and USB attached nShield devices, included in hwsp for Linux. |
| javasp | nShield Java | nCipherKM JCA/JCE Provider, associated classes (including nFast Java generic stub classes) and the KeySafe application. |

| Linux Package | Windows Feature in the Installer | Content |
|---|---|---|
| `jd` | nShield Java Developer | Java developer libraries and documentation for the nCore API and generic stub. |
| `ncsnmp` | nShield SNMP | nShield SNMP service and tools. |
| N/A | nShield Remote Administration Client Tools | Remote Administration Client tools and shortcuts. |
| N/A | nShield Trusted Verification Device | Driver for the Trusted Verification Device (TVD), included in `ctls` for Linux. |
| `raserv` | nShield Remote Administration Server | nShield Remote Administration server for enabling communication between remote clients and their Type3 smartcards and this machine. |

## 14.2. Components required for particular functionality

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

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

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

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

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

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

### 14.2.1. KeySafe

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

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

If you require the Microsoft CAPI CSP, you must install the nShield CSPs (CAPI, CNG) com-

ponent.

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

- The appropriate *nShield Connect User Guide*.
- The appropriate third-party integration guide for your application.

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

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

## 14.3. nCipherKM JCA/JCE cryptographic service provider

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

- The nShield Java bundle.

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

See the *nShield Connect User Guide* for more about configuring the nCipherKMJCA/JCE cryptographic service provider.

## 14.4. SNMP monitoring agent

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

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

```
If this is a first time install, the nShield SNMP Agent will not run by default.
```

```
Please see the manual for further instructions.
```

See the *nShield Connect User Guide* for more about how to activate the SNMP agent after installation.

# 15. Valid IPv6 Addresses

This appendix provides a list of valid IPv6 addresses for each of the types of addresses recognized by certain parts of the system. For information on setting up IPv6 addresses, see Configuring the Ethernet interfaces - IPv4 and IPv6 .

| Address type | Address Range (inclusive) (From \| To) | | Example |
|---|---|---|---|
| Unspecified | :: | :: | :: |
| Loopback | ::1 | ::1 | ::1 |
| Local Unicast | fc00:: | fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff | fdf8:f53b:82e4::53 |
| Link-local | fe80:: | febf:ffff:ffff:ffff:ffff:ffff:ffff:ffff | fe80::200:5aee:feaa:20a2 |
| Site-local (depreciated) | 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:fdd2 |
| 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 |

🛈 | The available addresses in the Global Unicast range are not contiguous.