Entrust nShield® 5c Quick Start Guide

This guide shows how to set up an nShield 5c, with or without access to an installed nToken client, on a Remote File System (RFS) machine for the first time. For more detailed information about setup procedures and options, see the *Entrust nShield 5c Installation Guide* and the appropriate chapters of the *Entrust nShield 5c User Guide*.

Check the physical security of the nShield 5c

See the *Entrust nShield Connect Physical Security Checklist* provided in the box with an nShield 5c and in the document folder on the installation media.

Install and configure an nToken to act as a client (Optional)

If you intend to use an nToken in another machine to act as a client for the nShield 5c, you can choose to install and configure the nToken now. This process is described in the *nToken Installation Guide*. The IP address of the nToken client will be used later, to add a new client to the nShield 5c.

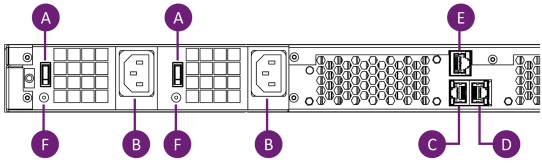
Install and physically connect the nShield 5c

1. **To install the nShield 5c in a 19" rack**, follow the instructions supplied with the Entrust nShield Connect Slide Rail Kit.

   To install the nShield 5c 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 as a guide to placing the feet. Then place the nShield 5c in its required location.

2. On the rear of the nShield 5c:

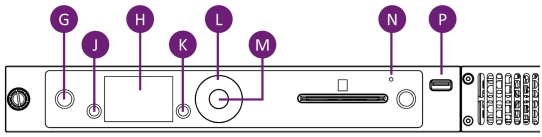
   - After ensuring the rocker switches (A) for both power sockets are set to OFF, connect the two power cables (B). The green lights will illuminate, indicating that power is available even though the unit is OFF.
   - Connect the Ethernet cable for the main subnet to the lower-left Ethernet port (C). Optionally, connect the Ethernet cable for a secondary subnet to the lower-right Ethernet port (D).
   - If you are using a rack with a serial port aggregator, connect the Ethernet cable from the aggregator (make a note of the port number) to the serial console port (E).
   - Set both rocker switches (F) to ON. The nShield 5c will power up.



3. On the front of the nShield 5c:

   - The power switch (G) flashes blue until the boot sequence completes. It then shows solid blue.
   - The details of the boot sequence appear on the screen (H).

     You interact with the screen using the options buttons (J, K), the scroll wheel (L) and the select button (M).
   - The status LED (N) shows steady blue after the boot completes, and then varies with activity.
   - Optionally, connect a keyboard to the USB serial console port (P).
     This enables you to bypass the option buttons (left/right arrow), the scroll wheel (up/down arrows) and the **Select** button (**Enter**). Numbers can be typed directly.



Configure the network connectivity for the nShield 5c

There are two methods to configure the nShield 5c network connectivity:

- Using the front panel of the nShield 5c.
- Using a serial console command line via the serial port aggregator.

NOTE - This guide includes commands/options to configure IPv4 networking. IPv6 networking is also supported.

To configure network connectivity using the front panel:

1. Using the front panel screen and controls (or keyboard), set the IP address for your primary subnetwork:

   System (1) > System configuration (1-1) > Network configuration (1-1-1) > Set up interface #1 (1-1-1-1) > Configure #1 IPv4 (1-1-1-1-1) > Static IPv4 address (1-1-1-1-1-2).

   Enter the IP address and subnet mask, confirm the details, and finish.

2. Set the default gateway IP address for your primary subnetwork:

   System (1) > System configuration (1-1) > Network configuration (1-1-1) > Set default gateway (1-1-1-4) > IPv4 Gateway (1-1-1-4-1).

   Enter the IP address, confirm the details, and finish.

3. If you want to set a network bond, routing tables, or IPv6 compliance, see the *nShield 5c Installation Guide.*

To configure network connectivity using the serial console command line:

1. Log in to your aggregator interface. Refer to the aggregator documentation for details.
2. In the aggregator interface, access the configuration for the aggregator port to which your nShield 5c is connected, and ensure that SSH connections are permitted to the port.
3. Start your chosen SSH software and start an SSH session to the port on the aggregator.
4. Enter credentials for the aggregator, and then enter credentials for the nShield 5c, see the *nShield 5c User Guide*.
5. Change your password if prompted. The serial console command line appears.
6. Optionally, type **?** and press **Enter** to list all serial console commands.
7. Set the IP address for the nShield 5c on your primary network (interface 0) using the following serial console command:

   netcfg iface=0 addr=<5c_ip_addr> netmask=<netmask>

8. Set the default gateway using the following serial console command:

   gateway <gateway_ip_addr>

Create and configure the Remote File System for the nShield 5c

Each nShield 5c must have a single Remote File System (RFS) configured. This stores master copies of all the files that the nShield 5c needs. The RFS can be on any machine in the same network as the nShield 5c. You will be able to access the nShield 5c via any client that is configured on the nShield 5c. See the *nShield 5c Installation Guide* for more information about the RFS.

To create the RFS for the nShield 5c, you must use Security World software commands:

1. Log in to the machine/VM which you want to act as the RFS and access a command prompt.
2. Determine the Electronic Serial Number (ESN) and hash of the nShield 5c using the following Security World command:

   anonkneti <5c_ip_addr>

   The ESN and hash are displayed.

3. Set up the RFS using the following Security World command:

   rfs-setup <5c_ip_addr> <5c_esn> <5c_hash>

   For this command, **<5c_esn>** and **<5c_hash>** are outputs from the **anonkneti** command.

There are two methods to configure the RFS for the nShield 5c:

- Using the front panel.
- Using the serial console command line.

To configure the RFS for the nShield 5c using the front panel:

1. Using the front panel screen and controls (or keyboard), set the IP address for the machine/VM containing the RFS:

   System (1) > System configuration (1-1) > Remote file system (1-1-3)

   Enter the IP address and port number. **NOTE** - This port must be open on the machine/VM's firewall.

   Choose if you want to enable config push on the RFS. See the *nShield 5c Installation Guide* for details.

   Choose if you want to enable secure authentication on the RFS and configure if required. See the *nShield 5c Installation Guide* for details.

   Confirm the details and finish.

2. Enable the client auto push feature from the nShield 5c to a configured nToken client:

   System (1) > System configuration (1-1) > Config file options (1-1-6) > Setup auto push (1-1-6-2) > auto push mode (1-1-6-2-1)

   Enable auto push mode, and then configure auto push mode.

   System (1) > System configuration (1-1) > Config file options (1-1-6) > Setup auto push (1-1-6-2) > Push address (1-1-6-2-2)

   Enter the IP address of the client, confirm the details, and finish.

3. Configure log file storage options:

   System (1) > System configuration (1-1) > Log config (1-1-7)

   Select **Append** to store logs on both the nShield 5c and the RFS or select **Log** to store on the nShield 5c only.

   Select the frequency of log saves (in minutes), confirm the details, and finish.

4. Optionally, set the date and time on the nShield 5c:

   System (1) > System configuration (1-1) > Date/time setting (1-1-8)

   Set the date and time, confirm the details, and finish.

To configure the RFS for the nShield 5c using the serial console command line:

1. From any machine in the network, start an SSH session to the serial port aggregator, and access the serial console command line.
2. Set the IP address for the machine/VM containing the RFS using the following serial console command:

   rfsaddr <rfs_ip_addr>:<port>

3. Enable client auto push between the client and the nShield 5c:

   push ON <client_ip_addr>

4. Configure log storage by referring to the *nShield 5c User Guide*. This cannot be done using the serial console.
5. Optionally, set the date and time on the nShield 5c:

   date [MMDDhhmm[YYYY][.ss]]

   Set the date and time, confirm the details, and finish.

Enrol a client on the nShield 5c

You must now teach the nShield 5c about a client, and then enrol that client on the nShield 5c.

NOTE - You can also enrol a machine that does not contain an nToken as a client if it is on the same network as the nShield 5c. However, the client will use software authentication. For full details, see the *nShield 5c Installation Guide*.

To teach the nShield 5c about a client, use the front panel:

1. Using the front panel screen and controls (or keyboard), add a new client:

   System (1) > System configuration (1-1) > Client config (1-1-4) > New client (1-1-4-1)

   Enter the client IP address and continue.
2. Choose if you want to store the client IP address in the config file. For a dynamically-allocated IP address on the client, you will typically reply **No** and continue.
3. Select your required permissions. The default is **Unprivileged**. If you want a privileged connection to the client, select **Priv. on any port**.
4. Choose if you want secure authentication enabled on the client, and configure as described in the *nShield 5c Installation Guide*.
5. If you selected secure authentication, enter the port number for the client, and continue.

   The nShield 5c will search for the client and display an nToken ESN and/or a software key.
6. Choose either the nToken ESN or the software key. A hash is displayed for your selection.
7. Leave the information on screen and enrol the client as described below.

To enrol an nToken client on the nShield 5c, you must use Security World software commands:

1. Log in to the nToken client machine and access a command prompt.
2. Retrieve the client ESN and client hash from the client using the following Security World command:

   ntokenenroll --hashes

   This command produces output that includes the nToken ESN and the hash for the nToken.
3. Return to the nShield 5c front panel and confirm the hash displayed there matches the nToken hash.
4. Enrol the client into the nShield 5c using the following Security World command:

   nethsmenroll --ntoken-esn <ntoken_esn> --privileged <5c_ip_addr> <5c_esn> <5c_hash>

   In the above command, **--privileged** is optional.

To enrol a non-nToken client on the nShield 5c, you must use Security World commands:

1. Log in to the machine/VM containing the client and access a command line.
2. Retrieve the client hash using the following Security World command:

   enquiry -m0

   This command produces output that includes the **kneti hash** for the client.
3. Return to the nShield 5c front panel and confirm the hash displayed there matches the **kneti hash**.
4. Enrol the client into the nShield 5c using the following Security World commands:

   nethsmenroll --privileged <5c_ip_addr> <5c_esn> <5c_hash>

   In the above command, **--privileged** is optional.

For all client types:

1. Retrieve details for all installed modules using the following Security World command:

   enquiry
2. Confirm that the command output includes a module section for the nShield 5c. The section will list the nShield 5c ESN and indicate an operational state. For example:

   Module #1:

enquiry reply flags	**none**
enquiry reply level	**Six**
serial number	**<5c_esn>**
mode	**operational**

This completes the installation and essential configuration of the nShield 5c.

Product documentation

https://nshielddocs.entrust.com

