Entrust nShield® 5c 10G Quick Start Guide

This guide shows how to configure a 5c 10G and set it up on a KeySafe 5 machine for the first time. For detailed setup procedures and options, see the *Security World Software Installation Guide* at https://nshielddocs.entrust.com/.

Equipment required for the installation

Supplied with the 5c 10G by default:

- USB serial console cable.
  To configure the 5c 10G, you must use a serial console command line through the console port.
  The serial console port will operate at 115200 baud, 8 data bits, no parity, and 1 stop bit (115200/8-N-1).
  You can use a serial port aggregator or the serial session software of your choice.

Supplied with the 5c 10G if ordered:

- 2x Ethernet port devices: Small Form-factor Pluggable+ module.
  You need at least 1 SFP+ module to make the 5c 10G operational.

NOT supplied with the 5c 10G:

- KeySafe 5 client-side software (if you have no KeySafe 5 installation yet).
- 1x host to configure the HSM using the CLI - serial console command line (direct or through a switch).
- 1x server/VM for the KeySafe 5 installation (optional if you already have installed KeySafe 5).
- 1x server/VM to act as the client that will use the HSM.

Check the physical security of the nShield 5c 10G

See the *Physical Security Checklist* provided in the box with an 5c 10G or at https://nshielddocs.entrust.com/.

Identify the network settings for the 5c 10G

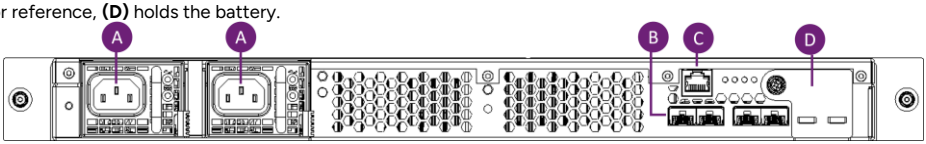
See *5c 10G network profiles* in the *nShield Hardware Install and Setup Guide* at https://nshielddocs.entrust.com/.

Install and physically connect the nShield 5c 10G

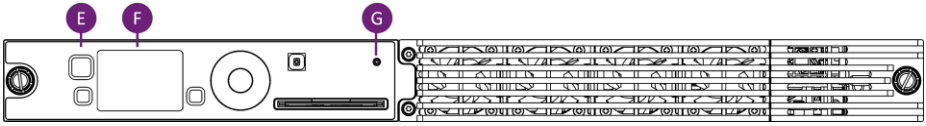
1. Install the nShield 5c 10G in a 19" rack.
   Follow the instructions supplied with the *Entrust nShield® Premium Slide Rail Kit*.
2. On the **rear of the nShield 5c 10G**, plug an SFP+ module into the leftmost SFP+ 10G port, Port 1 **(B)**.
3. Connect the network cable for the main subnet to make the HSM accessible from KeySafe 5.
4. Optionally, if your network settings require the 5c 10G to use additional SFP+ modules, plug them in to the other ports. If your network settings require a secondary subnet, connect a network cable to the relevant SFP+ module.
5. Connect the serial console cable from the serial console port **(C)** to the host running your serial session software. The connector can connect directly to your client machine or to a serial port aggregator for remote access.
6. Connect the two power cables to their sockets **(A)**.

The 5c 10G automatically powers up when it is connected to the power.

For reference, **(D)** holds the battery.



On the front of the 5c 10G, the stand-by button **(E)** flashes until the boot sequence completes and the details of the boot sequence appear on the screen **(F)**. The status LED **(G)** shows steady blue after the boot completes and then varies with activity.



Configure the network connectivity

DHCP is supported, and if you have the 5c 10G connected to a DHCP server, it will automatically pick up an address on boot once the network services are up. To configure network settings manually, you must use the serial console command line interface (CLI) via the serial console port.

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

To configure network connectivity manually using the serial console CLI:

1. Open a serial session that connects to the serial cable port interface.
2. Once connected, log in as the **cli** user.
3. The default password is **admin**. Change the password when prompted. The new password must be at least 8 characters long.
4. Set the IP address for the 5c 10G on your primary network (eno1):
   netcfg static -a <5c-10G-ip-addr/prefixlen> -g <gateway>
   For example:
   netcfg static -a 192.168.10.5/24 -g 192.168.10.1
5. Ensure that you can ping your KeySafe 5 Service machine before proceeding.

Install KeySafe 5

Each 5c 10G must be configured on a KeySafe 5 deployment. The KeySafe 5 deployment is used to manage the 5c 10G. The KeySafe 5 deployment can be on any machine in the same network as the 5c 10G. You will be able to access the 5c 10G via any client that is configured on the 5c 10G.

Skip this section if you already have a compatible KeySafe 5 deployment in place. For compatibility information, see the *nShield Security World Release Information*.

1. Log in to the machine or VM on which you want to install KeySafe 5.
2. Install the latest version of the Security World software as described in the *Security World Software Installation Guide*.
3. Open the following ports on the firewall, TCP and inbound only:
   18080 - loopback (localhost) interface, only accessible to the browser directly on the node where KeySafe 5 is running
   18084 - NATS message bus server embedded in the KeySafe 5 agent management service, for local use on the node
4. Download the KeySafe 5 server installation file from Entrust support website and transfer the file to the machine.
5. Perform the installation. Replace **1.2.3** in the following commands with the KeySafe 5 version.

   On **Windows**:
   a. Extract the **nshield-keysafe5-1.2.3.tar.gz** to an appropriate location.
   b. In the **keysafe5-service** folder run the **keysafe5-server-1.2.3-windows.msi** to install the service.
   c. Confirm the nShield KeySafe 5 service is running via Windows Services.

   On **Linux**:
   a. Create a directory and download/paste the KeySafe 5 package into it, for example, **mkdir /tmp/ks5Download**.
   b. **cd /**
   c. **sudo tar -C / -xzvf /tmp/ks5Download/nshield-keysafe5-1.5.0.tar.gz**
   d. **sudo tar -C / -xzvf /keysafe5-service/keysafe5-server-1.5.0-Linux.tar.gz**
   e. **sudo /opt/nfast/keysafe5/server/sbin/install**
6. Check that you can access the KeySafe 5 webUI by opening a browser inside the KeySafe 5 server to the following address:
   https://127.0.0.1:18080

Create and configure the 5c 10G in the KeySafe 5 webUI

1. Check the date and time to prevent validity issues with the certificate that will be created during the configuration.
   (cli) datetime
   The date and time reported by **datetime** need to match the date and UTC time on your PKI infrastructure.
   To correct the date or time, use the following command:
   (cli) datetime -D <YYYY-MM-DD hh:mm:ss>
   Use the 24-hour clock for the UTC time.
2. Configure the 5c 10G KeySafe 5 agent through the serial console command line.
   (cli) ks5agent cfg message_bus.url=<KeySafe-5-IP-addr-IPv4>:18084

   If you are using IPv6, you must use the square brackets around the address:
   (cli) ks5agent cfg message_bus.url=[<KeySafe-5-IP-addr-IPv6>]:18084
3. Restart the KeySafe 5 agent when prompted.
   Restart KeySafe 5 agent to apply new configuration (y|n): y
   Restarting KeySafe 5 agent.
   Success.
4. Verify the configuration.
   (cli) ks5agent cfg
   Ensure the message bus settings reflect the changes.
5. Generate a Certificate Signing Request in the 5c 10G CLI using **mbcsr**. The output will be a CSR in PEM format.
   (cli) ks5agent mbcsr
6. Save the entire output as a new file called **tls.csr**. Make sure you include the following lines:
   -----BEGIN CERTIFICATE REQUEST -----
   -----END CERTIFICATE REQUEST--------
7. Copy the **tls.csr** to your issuing Certificate Authority and sign it.
8. After it has been signed, copy the signed **tls.crt** file to the KeySafe 5 agent server.
9. Export the issuing Certificate Authority certificate, rename it to **ca.crt**, and copy it to the KeySafe 5 agent server.
10. Encode the **tls.crt** and **ca.crt** files to Base64:
    base64 --wrap=0 ca.crt
    base64 --wrap=0 tls.crt

    TIP: If you are using the KeySafe 5 demo CA, you can sign the CSR as follows:

    a. Transfer the **ks5-agent.csr** file to the KeySafe 5 machine.

    b. Run **keysafe5-server-admin**:
       On Linux:
       sudo /opt/nfast/bin/keysafe5-server-admin sign ks5-agent.csr
       On Windows, from an Administrator Command Prompt:
       "C:\Program Files\nCipher\nfast\bin\keysafe5-server-admin.exe" sign ks5-agent.csr

       The **tls.crt** and **ca.crt** files are generated in this directory.
       Use the Base64 strings from these **tls.crt** and **ca.crt** files in the next step.
11. Install certificates on the 5c 10G.

    In the 5c 10G CLI, install the certificates. Copy the Base64-encoded strings for the tls.crt and ca.crt and use them in the commands below:
    (cli) ks5agent mbtls tls.crt <Base64-encoded-TLS-string>
    (cli) ks5agent mbtls ca.crt <Base64-encoded-CA-string>
    Use the Base64-encoded strings that you generated during signing in the previous step.
9. Restart the KeySafe 5 agent on the 5c 10G.
   (cli) ks5agent restart
   Restarting KeySafe 5 agent.
   Success.
10. Check the KeySafe 5 webUI and see if the 5c 10G has connected. If successful, it will have a **HEALTHY** status.
    If you don't see the HSM listed or its status is not HEALTHY, check the logs for possible issues:
    (cli) ks5agent log

Set up the tenancy in KeySafe 5 to enable access to the HSM from KeySafe 5

1. In the KeySafe 5 webUI, select **Hardware Management > HSMs** and select your 5c 10G HSM.
2. Select **Tenancies > Download CSR**.
3. Sign the CSR with your PKI infrastructure. If you are using the KeySafe 5 demo CA, follow **step 7** in *Create and configure the 5c 10G in the KeySafe 5 webUI* of this guide. The tenant CSR is called **certificate.csr** when you download it from KeySafe 5.
4. Select **Tenancies > Configure**.
5. Change the default (127.0.0.1) value for **Central Platform Address** to the IP address of the KeySafe 5 server (XXX.XXX.XXX.XXX:18084):
    a. Enable Auto Start.
    b. For the KeySafe 5 agent certificate, use the **tls.crt** file, for the CA certificate, use the **ca.crt** file.
    c. Select **Confirm**, close the dialog with **Close**, then select **Start**.
    d. Select **Confirm** again to start the tenancy.
6. Check the tenancy: Select **Hardware Management > HSMs.** You should see 2 HSMs with the same ESN. The one with the VCM is the tenant HSM. The other one is the platform HSM.

The system is now ready for client configuration.

Add the client in the KeySafe 5 webUI

1. Select **Hardware Management > HSMs** and select the tenant HSM you want to use.
   The tenant HSM is the HSM displayed with the VCM.
2. Select **Clients > Add New Client**.
3. In **Client Configuration**, select the **Client Permission** type, and for **Client Authentication** enter the IP address and the KNETI hash of the client.
   If you need to retrieve the KNETI hash, run **enquiry -m0** on the client and look up the KNETI hash in the output.
4. Select **Save** then select **Close**.

The HSM is ready to be configured in the client.

Enroll the 5c 10G HSM to the client

1. Log in to the machine/VM client you want to enroll the HSM to.
2. Install the latest version of the Security World software as described in the Installation Guide for the HSM.
3. Determine the Electronic Serial Number (ESN) and KNETI hash of the 5c 10G using the following Security World command:
   anonkneti <5c-10G-ip-addr>
   The output will contain the ESN and the KNETI hash, for example:
   876E-A9E8-FBEA c766ea7e75316fbec11f8354917f4ca54f3b9cc0
4. Enroll the HSM:
   sudo /opt/nfast/bin/nethsmenroll --privileged <5c-10G-ip-addr> <5c-10G-ESN> <5c-10G-KNETI>
5. Check that the HSM has been enrolled. Run:
   enquiry
6. The HSM should be listed in the module section of the output, it should be in **operational** state, and the hardware status should be **OK**.
   For example:
   Module #1:
   enquiry reply flags none
   enquiry reply level Six
   serial number <5c-10G-ESN>
   mode operational
   [...]
   hardware status OK

This completes the installation and essential configuration of the 5c 10G and it will appear in an enquiry output in the security world. However, you won't be able to perform any security world operations with the 5c 10G from KeySafe 5 until you install and set up a KeySafe 5 agent on your security world client. For instructions for that, and for details on configuration options, see the KeySafe 5 user documentation at https://nshielddocs.entrust.com/.