

Entrust nShield HSM Integration Guide

Prerequisites:

1. Cloud Client Software Setup:

Note: If you are setting up an on-premises HSM, skip to prerequisite step 2.

- a. Download the Client Software from the Entrust Support Portal.
 - b. Unzip the zip file.
 - c. Run the installer as an administrator.
 - d. Select Client Installation only.
 - e. Unpack and Configure the Cloud HSM Bundle which should include:
 - i. nshield-cloud.conf
 - ii. cloud.cert
 - iii. client.key
 - iv. client.cert
 - v. Optionally: module.nkn, module.dns
 - f. Place them in the **C:\ProgramData\nCipher\Security World\cloud**
2. On-Premises HSM Client Software Setup
 - a. Download the Client Software from the Entrust Support Portal.
 - b. Unzip the zip file.
 - c. Run the installer as an administrator.
 - d. Select the options you need to install.

1. Security World Configuration

1. The following steps require access to an elevated command prompt or root.
2. Test access to nSRES with the following command:

anonkneti --port 9014 [Assigned HSM IP Address]

Note: To check the version of security world installed on the client issue the following command.

anonkneti -v

Entrust recommends using the latest Security World Client for integration testing.

3. The command should return two numbers, a Serial Number (ESN) and KNETI HASH.

[ESN] [KNETI HASH]

4. Export the world and module files from the email and into the Security World client's **kmdata/local** folder:

- **Windows** - C:\ProgramData\nCipher\Key Management Data\local
- **Linux** - /opt/nfast/kmdata/local

5. If switching to new nSRES – nSRTL module(s) you must unregister the previous module(s).

nethsmenroll --remove --port (Port Assignment) [Assigned HSM IP Address] ESN KNETI-HASH

6. To enroll, use the following command for each ip address:

nethsmenroll --port 9014 [Assigned HSM IP Address]

Note: Repeat steps 1-6 above as necessary to enroll each IP address for HA testing.

7. To test HSM connectivity, use the following diagnostic command(s):

enquiry

Note: enquiry will confirm that the module is connected and provide a list of available nShield features.

and/or

nfkminfo

Note: nkfminfo will display information about the Security World.

8. To test benchmarking and verify the consistency of the Security World, use the following command(s):

perfcheck -m1 signing:287

Note: perfcheck performs a test of the module.

and/or

nfkcheck

Note: nfkmcheck will check the consistency of the Security World data.