Quintessence Labs

Data Uncompromised

nCipher nShield Connect HSM
Initial Setup Guide
qCrypt KMS software 1.9

QuintessenceLabs Contact Details

Australian HQ	Unit 1 Lower Ground 15 Denison Street, Deakin, ACT, 2600. Telephone: +61 2 6260 4922 Fax: +61 2 6260 5011
USA Office	175 Bernal Road Suite 220 San Jose, California, 95119. Telephone: +1 650 870 9920 Fax: +1 650 870 9902
Email	info@quintessencelabs.com
Website	www.quintessencelabs.com

Disclaimer

Contents

1 Introduction

This document applies to the following product variants : qCrypt 200V, qCrypt 250A and qCrypt 300R.

It applies to you if your qCrypt appliance does not have an in-built HSM and you wish to connect it to an external nCipher nShield Connect network HSM. It is assumed that the nCipher nShield Connect HSM is initially in its factory state and you have physical access to the network HSM.

This guide shows the necessary steps to set up a default configuration. It should be used in conjunction with your nCipher nShield Connect documentation.

This document was written for and tested on:

Client Software Version	Module Version
12.40.2	3.4.2

The main steps to connect your qCrypt appliance to an external nCipher nShield Connect HSM are:

1. Prepare nCipher nShield Connect HSM[1]
2. Setup Remote File System (RFS) and HSM[1 2]
3. Create security world[1]
4. Configure qCrypt and HSM configuration
5. Setup Cooperation client[3] (optional)

NOTE: Unless otherwise specified, the terms 'HSM' and 'network HSM' in this guide are used to refer to the nCipher nShield Connect network HSM.

[1] To perform these steps please refer to instructions included in the nCipher documentation.
[2] This step is optional from the point of view of the qCrypt appliance. However, it does provide a number of administrative / provisioning features that the user may find useful.
[3] This step is only possible if a RFS has been configured.

1.1 Prerequisites

You will need:

- nCipher nShield Connect HSM setup with a security world (see steps above).
- Access to the **security world file**.
- Access to the **module file**.
- Access to the qCrypt appliance.
- A HSM smart card reader connected to the network HSM with an Administrator Card Set (ACS) card in the card reader.
- Appropriate version of the qCrypt installation tarball from the download site:

  https://download.quintessencelabs.com/

WARNING: The HSM cannot be used without completing the setup procedure.

2 Setup qCrypt appliance to use nCipher nShield Connect HSM

2.1 Setup HSM for qCrypt clients

The HSM must be configured to recognize the qCrypt appliance as a client.

NOTE: The notes below assume that a RFS has been setup. If this is not the case, refer to nCipher documentation for information on configuring HSM clients.

Login into the RFS server as root. You will need `/opt/nfast/bin` in your PATH.

2.1.1 Edit the HSM Configuration

- Copy the default configuration file. In the `/opt/nfast/kmdata/hsm-xxxxx-xxxx/config/` folder (where the `xxxxx-xxxx` section will vary):

```
cp ./config ./config.new
```

- Add qCrypt (i.e. HSM client) IP addresses to the `[hs_client]` section of the `config.new` file:

```
[hs_clients]
addr=192.168.3.130
clientperm=priv
-----------------------------------
addr=192.168.3.133
clientperm=priv
```

NOTE: lines of dashes ('---') can be used to separate multiple clients. In the example above, 192.168.3.130 and 192.168.3.133 are two qCrypt clients of the HSM.

2.1.2 Push new configuration to the network HSM

```
cfg-pushnethsm --address=<HSM-IP> config.new
```

This command updates the HSM's configuration. The original `config` file on the HSM should update automatically after a few seconds. Please ensure that the `config` file has indeed been updated.

2.2 Setup qCrypt client for HSM

This step sets up a qCrypt appliance so it can be used as a client of the network HSM.

This step involves installing HSM Client software on the qCrypt applicance then setting up a **softcard** to allow access to the HSM.

2.2.1 Install HSM Software on qCrypt

- Download the appropriate[1] version of the qCrypt installation package tarball from the download server at:

  https://download.quintessencelabs.com/

- Verify that the downloaded package checksum matches the displayed checksum on the download server.
- Copy the qCrypt installation package tarball to the qCrypt appliance `/home/service` folder.
- Login to the qCrypt appliance via the console as root user, or SSH in as `service` user then elevate to root.
- As `root`, untar the qCrypt installation package tarball and enter the installation folder.

```
tar xf 0004263-kms-1.9.tar.bz2
cd 0004263-kms-1.9
```

  The tarball and folder names above are examples only, and will change for different versions of qCrypt.

- Run the install command as root user, with the following arguments:

```
./install.sh --network-hsm hsm_nshield_connect
```

This command will install necessary software to enable the qCrypt appliance to connect to the network HSM.

2.2.2 Create softcard and Setup Master Encryption Key provider

The **softcard** is a persistent logical token, protected by a passphrase. The softcard is used by the qCrypt appliance to access the HSM. Two softcards on different qCrypt appliances can have the same name and passphrase, but will have different (unique) hashes.

You will need the following prerequesites to continue with this step:

[1] The version should correspond to the currently running qCrypt software. The current version can be viewed via: **User Icon** | **About System**

- Security world is created.
- **Security world** and **module** files have been copied to the qCrypt applicance. If a RFS machine has been configured, the two files can be found in `/opt/nfast/kmdata/local/`.

> **CAUTION:** Do not rename the **security world file** or **module file**, when transferring to the qCrypt applicance.

- qCrypt has nShield Connect software installed on it. (See **Section 2.2.1 Install HSM Software on qCrypt**).
- An Administrator Card Set (ACS) card is in the card reader.
- The qCrypt IP address is configured as a client of the HSM.

Run the setup wizard:

```
/root/hsm_tools/setup_nshield_connect.py
```

This will enrol the HSM, create a softcard, and set up the HSM as a Master Encryption Key (MEK) provider for qCrypt.

The script will request the following information:

- ip address or hostname of the HSM (192.168.60.140 in examples)
- full path and name of the **security world file**
- full path and name of the **module file**
- softtoken name (new or existing name entered by user)
- softtoken password/passphrase (entered twice, for confirmation, by user)

The wizard will create one softcard with a passphrase for qCrypt to use. If the wizard completes successfully, you see the HSM listed as a cryptographic provider in the **Crypto Providers**/**Cryptographic Providers** tab on the Web Interface of the qCrypt appliance. This allows the configured HSM to provide master encryption keys to the qCrypt appliance. Please see the Cryptographic Providers section of the qCrypt User Guide for further details.

3 Setup Cooperation Client (optional)

> **TIP:** This step is only applicable if a RFS has been configured.

Setting a client up as a 'cooperation client' allows it to sync or commit data to or from an RFS machine automatically. If a client is not a cooperation client, any card, module, or key files must be copied manually from the RFS or other clients.

1. On the RFS machine, enable client as 'gang-client':

   ```
   rfs-setup --force --gang-client --write-noauth <IP>
   ```

   where <IP> is the IP address of the qCrypt appliance.

   This command will inform the RFS server that the qCrypt appliance at <IP> is a cooperation client.

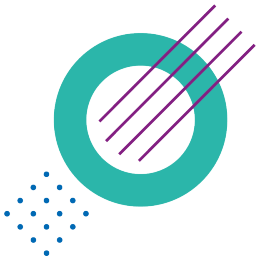
2. On the qCrypt appliance, setup RFS:

   ```
   cd /opt/nfast/bin/
   ./rfs-sync --no-authenticate --setup <RFS-IP>
   ```

   This command instructs the qCrypt client machine to use the RFS machine at <RFS-IP> as an RFS.

3. On the qCrypt applicance, update data from RFS:

   ```
   ./rfs-sync -U
   ```



Quintessence Labs

Data Uncompromised

AUSTRALIA
Unit 1, Lower Ground
15 Denison St
Deakin, ACT 2600
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com
info@quintessencelabs.com

Document ID: 4421