www.EncryptionConsulting.com

PROTEGRITY & NSHIELD CONNECT INSTALLATION/ INTEGRATION PROCEDURES

DOCUMENT INFORMATION

Prepared By:	**Puneet Singh**
E-mail:	**PuneetSingh@EncryptionConsulting.com**
Reviewed/Approved By:	
Create Date:	**3rd July 2020**
Version:	**1.0**
Updated:	

Version History			
Version	**Author**	**Date**	**Revision Notes**
1.0	Puneet Singh	7/3/2020	
1.2	Daniel Pintal	10/22/2020	Entrust nShield revision

Table of Contents

INTRODUCTION

This Document covers basic installation and setup of the nShield Connect and Security World Client configuration. For more detailed instructions please refer to the *nShield Connect User Guide*.

Note:
nCipher is now Entrust Data Protection Solutions.

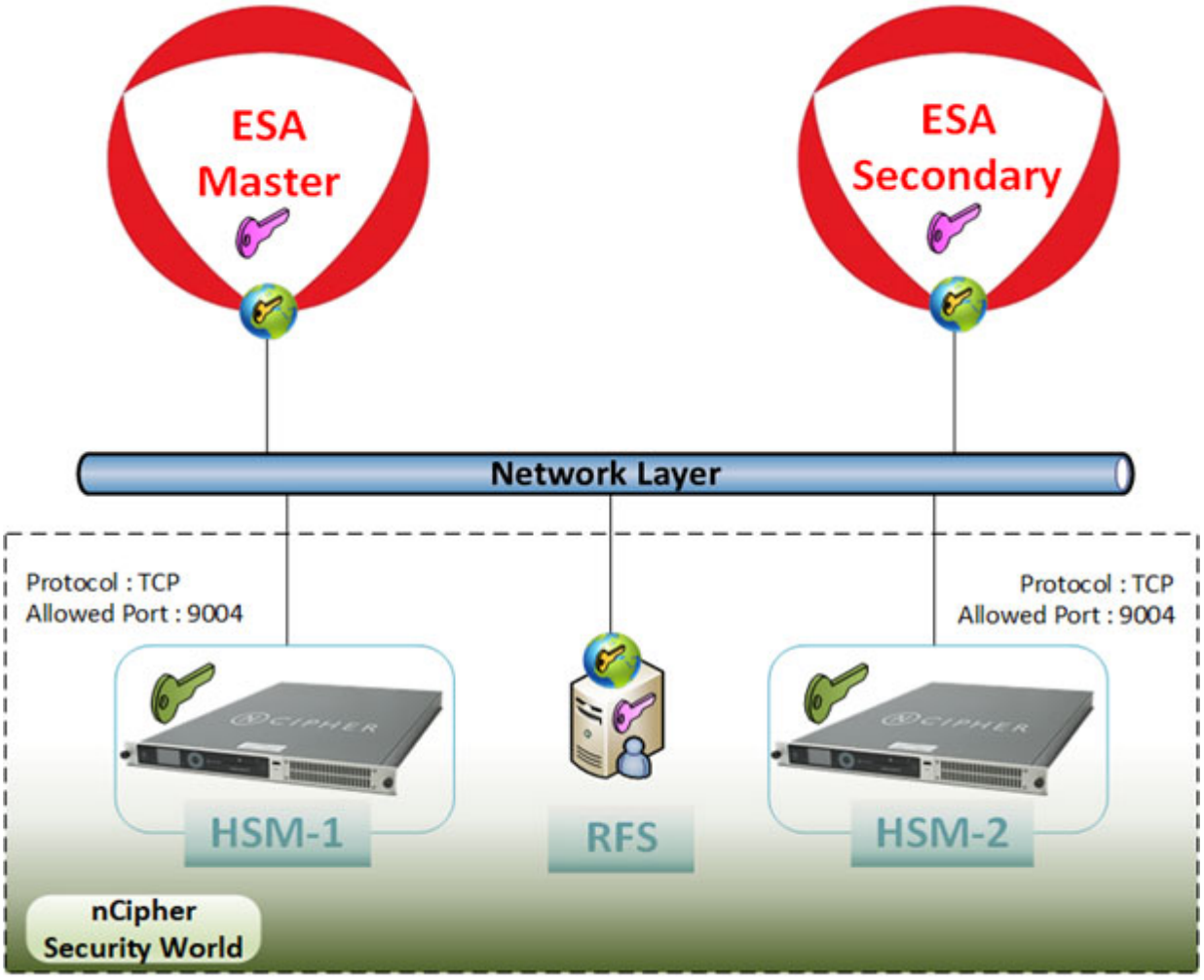
This document is an addendum to the Entrust nShield User Guides.

nShield, nShield Connect are synonymous with the Entrust nShield.

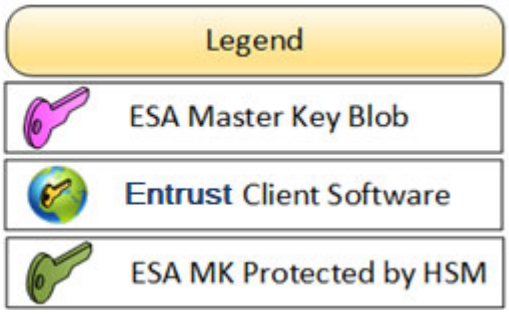
Note: The enquiry mode output of Module #1 and Module #2 should be **operational,** and the reply flags should be **none** before proceeding.

```
root@ESA1:/opt/nfast/bin# ./enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        8704-03E0-D947
 mode                 operational
 version              12.40.2
 speed index          478
 rec. queue           110..208
 level one flags      Hardware HasTokens
 version string       12.40.2+ main ddb26e9ca81bc44e9c2cbf5e336e693f9740f12f nsh
ield/nshield-project , 3.4pla2 Built on Apr 30 2018 11:22:00, Bootloader: 1.2.3,
 Security Processor: 2.1.18 , 12.45.2+ main 0ec1a5bcdb84d83f31724ebd33ecef471515
215c nshield/connect-project
 checked in           0000000059d623fa Thu Oct  5 07:22:18 2017
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
ollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp Ha
sLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds JobFragmentation LongJobsPr
eferred Type2Smartcard ServerHasCreateClient HasInitialiseUnitEx Type3Smartcard
HasKLF2
 module type code     0
 product name         nFast server
 device name
 EnquirySix version   4
 impath kx groups
 feature ctrl flags   none
 features enabled     none
 version serial       0
 remote server port   9004

Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        8704-03E0-D947
 mode                 operational
 version              3.4.2
 speed index          478
 rec. queue           22..50
 level one flags      Hardware HasTokens
 version string       3.4pla2 Built on Apr 30 2018 11:22:00, Bootloader: 1.2.3,
Security Processor: 2.1.18 , 12.45.2+ main 0ec1a5bcdb84d83f31724ebd33ecef4715152
15c nshield/connect-project
 checked in           000000005ae73497 Mon Apr 30 10:21:59 2018
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
```

SYSTEM ARCHITECTURE



Entrust nShield requires an RFS (Remote File-System Server) to store the Security World Key and Client Keys blobs for backup, replication and to ease management of application keys including ESA Master Key.



REFERENCES

The following documents from Entrust should be referenced when using this addendum:

- nShield Connect User Guide
- nShield User Guide

All documentation is available to licensed Entrust nShield customers and is available electronically in PDF form from Entrust.

INSTALLATION PROCEDURE

The following procedures should be followed for the standard installation steps. For any support when executing these steps please contact Entrust nShield Customer Support.

STEP 1: What you need

Ensure that:

- The nShield Connect is safely and securely installed.
- The main cables and ethernet cable are securely fitted.
- The nShield Connect powers up successfully when you turn on the power supply.

Step 2: Installing the software

After installing the nShield, you must install the Security World Software on the client computer and the computer designated as your remote file system (RFS). For more information, see the nShield Connect User Guide.

Step 3: Basic software setup (Basic configuration of the nShield Connect)

This section describes how to set up the nShield for the first time using the default configuration file

Note 1: The following procedures assume that you have added the path **%NFAST_HOME%\bin** (Windows) system variable.

Note 2: Use Appendix-A (RFS) to Install the Security World Client on a Linux Environment. All other configuration pertaining to nShield Connect and client will remain the same as below.

To complete a basic configuration of the nShield Connect:

1. Install the Security World Software on the RFS and client machines.
   Note: Local Administrator privileges are needed on each machine.

2. Configure the Ethernet interface #1

   - From the front panel, select: (1-1-1-1-1-1) ***System > System Configuration > Network Config > Set up Interface #1 > Configure #1 IPv4 > IPv4 enable/disable > Finish***
   - Set up IPv4 Static Address: (1-1-1-1-1-2) ***System > System Configuration > Network Config > Set up Interface #1 > Configure #1 IPv4 > Static IPv4 address > Enter IPv4 Address > Enter the subnet mask > Select Next > Select Finish > Select Continue***
     - Note: Do not use the same subnet if both interfaces are used.
   - Then ***Reboot*** the nShield (1-6-2) ***System > Shutdown/Reboot > Reboot > Confirm***
   - Set the network location of the nShield by entering the default gateway (from menu 1-1-1-3-1).
     - ***System > System configuration > Network config > Set default gateway > IPv4 Gateway > Enter IPv4 Gateway > Select Next > Select Finish > Select Continue.***

3. Configure the RFS:
   - Retrieve the ESN and keyhash of the nShield by running the following command: ***anonkneti <nShield Connect IP>***

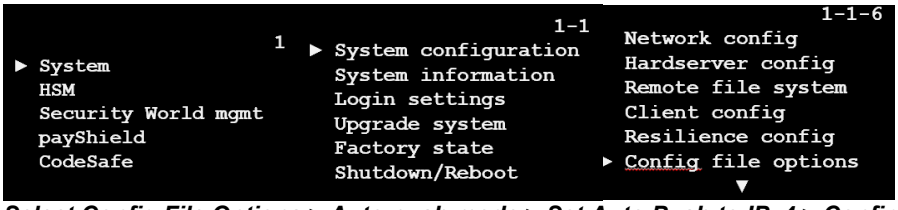
The ESN and keyhash are used in the command described in the next step.

- Create the directory structure on the RFS by running the following command: ***rfs-setup --force <nShield Connect IP> <nShield Connect ESN><nShield Connect KNETI HASH>***

```
C:\Program Files (x86)\nCipher\nfast\bin>anonkneti.exe 169.254.69.175
8704-03E0-D947 2cfcd629d9259c1aa8eca59611618b3852da38ac

C:\Program Files (x86)\nCipher\nfast\bin>rfs-setup 169.254.69.175 8704-03E0-D947 2cfcd629d9259c1aa8eca59611618b3852da38ac
Adding read-only remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\local exists
Adding new writable remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\hsm-8704-03E0-D947 exists
Ensuring the directory C:\ProgramData\nCipher\Feature Certificates exists
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\hsm-8704-03E0-D947\features exists
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\hsm-8704-03E0-D947\config exists
Ensuring the directory C:\ProgramData\nCipher\Log Files\hsm-8704-03E0-D947 exists
Saving the new config file and configuring the hardserver
Done
```

4. Configure the nShield to use the RFS (from menu 1-1-3-1): ***Select Define IPv4 RFS > Enter IP address of the RFS machine > leave port number as the default, 9004 > Select Continue > Select Finish***.

5. You can allow a configuration to be pushed automatically from the RFS to the nShield, or you can fetch the updated configuration manually from the nShield. The ***auto push*** feature allows future nShield configuration to be performed remotely (that is, without access to the front panel of the nShield).
   If you are planning to use Remote Administration, you should enable ***auto push*** on the nShield Connect, once you have configured the RFS (from menu 1-1-6-2-1):



   - ***Select Config File Options*** > ***Auto push mode*** > ***Set Auto Push to IPv4*** > ***Confirm > Continue***
   - (1-1-4-6-2-2) Select ***IPv4 Push address*** > ***enter the IP address of the RFS*** > ***Select Confirm > Continue***.
   - Add RFS as a client (from menu 1-1-4-1***) Select System > Select System Configuration > Client Config > Select New IPv4 client > Enter the RFS IP address > Select Next.***

6. Configure log file storage (from menu 1-1-7) by selecting one of the following options:

   - ***Append:*** stores the files on the nShield and RFS.
   - ***Log:*** stores the files on the nShield only.
     - We recommend ***selecting Append*** because if you select **Log** you can only view the log file from the nShield Connect front panel. Moreover, the log file stored on the nShield is cleared every time it is powered down
     - ***Select Append > Select Finish > Set time between each append to 1 min > Select Finish > Select Continue***

7. Set the time and date on the nShield as UTC (from menu 1-1-8) and then reboot.
   - ***Enter current UTC date > Select Next > Enter current UTC time > Select Finish > Select Reboot Now***

Step 4: Interfacing the nShield with a client

A Security World client is a machine using the nShield for cryptography.

To configure the nShield and client:

1. Configure the nShield to accept requests from the client machine:

   - (from menu 1-1-4-1***) Select System > Select System Configuration > Client Config > Select New IPv4 client > Enter the remote client IP address > Select Next.***
   - If you want a privileged connection to the client ***> select Priv. on any port***.
     - 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 Unix-based systems.
     - Priv. on any ports - Privileged connections are allowed on all ports.
   - If your client does not have an nToken that you want to use ***> select No for nToken > Select Next > Select Continue***.

2. Configure the client to forward cryptographic requests to the nShield Connect:

   - Retrieve the ESN and keyhash of the nShield by running the following command:
     anonkneti <nShield Connect IP>
     The ESN and keyhash are used in the command described in the next step.
   - Run the following commands:
     If you are enrolling the client without an nToken:
     nethsmenroll [Options] -p <nShield Connect IP> <nShield Connect ESN> <nShield Connect KNETI HASH>

```
C:\Program Files (x86)\nCipher\nfast\bin>anonkneti.exe 169.254.69.175
8704-03E0-D947 ffbe0ad463f59912c284fa9bf57b3aab106b242e

C:\Program Files (x86)\nCipher\nfast\bin>rfs-setup.exe 169.254.69.175 8704-03E0-D947 ffbe0ad463f59912c284fa9bf57b3aab106b242e
Adding read-only remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\local exists
Adding new writable remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\hsm-8704-03E0-D947 exists
Ensuring the directory C:\ProgramData\nCipher\Feature Certificates exists
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\hsm-8704-03E0-D947\features exists
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\hsm-8704-03E0-D947\config exists
Ensuring the directory C:\ProgramData\nCipher\Log Files\hsm-8704-03E0-D947 exists
Saving the new config file and configuring the hardserver
Done

C:\Program Files (x86)\nCipher\nfast\bin>nethsmenroll.exe -p 169.254.69.175
Remote module returned ESN: 8704-03E0-D947
                    HKNETI: ffbe0ad463f59912c284fa9bf57b3aab106b242e
Is the above correct? (yes/no): yes
OK configuring hardserver's nethsm imports
```

3. Configure the TCP sockets on the client for Java applications (for example, KeySafe) by running the command:
   config-serverstartup -s -p

4. Stop and restart the hardserver:

   On Windows: Run the commands:
   net stop "nfast server" (wait 30 seconds after command)
   net start "nfast server" (wait 30 seconds after command)

5. Test the completed installation by running the command:
   enquiry
   See Enquiry utility for an example of the output that the enquiry utility generates.

Step 5: Using a Security World

Before creating the nShield Security World, Open the cardlist file present at the following location and Enter the Admin card serial numbers.

Step1 : C:\ProgramData\nCipher\Key Management Data\config\cardlist
Step2: Add the ACS card serial numbers in cardlist file as shown in screen shot below

cardlist - Notepad

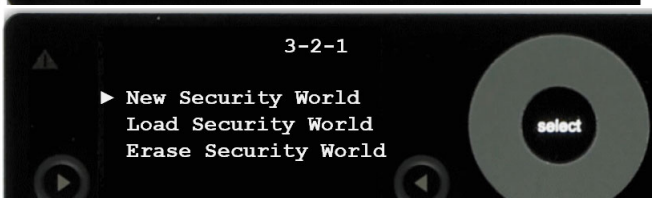
File Edit Format View Help

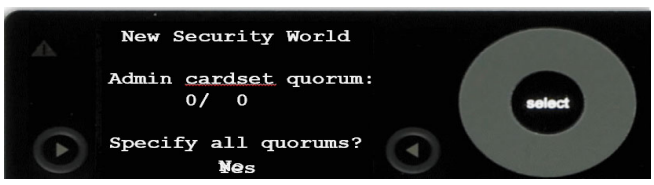
```
# This is the cardlist file, which contains the serial numbers of any
# Remote Administration Ready Smartcards that a system administrator
# has permitted to be used. These serial numbers are printed on the
# face of the smartcards
# Examples of valid 16 digit serial numbers:
#     XXXXXXXX-XXXXXXXX
#     XXXXXXXXXXXXXXXX
#     XXXX-XXXX-XXXX-XXXX
# To permit any cards presented to be used:
#      *
# The default configuration file has no cards listed, this means
# that all cards will be rejected by default.
5268047570068542
5268047570068543
5268047570068544
```

- Then clear the nShield for the changes to take effect by inputting the command ***nopclearfail –clear --all***

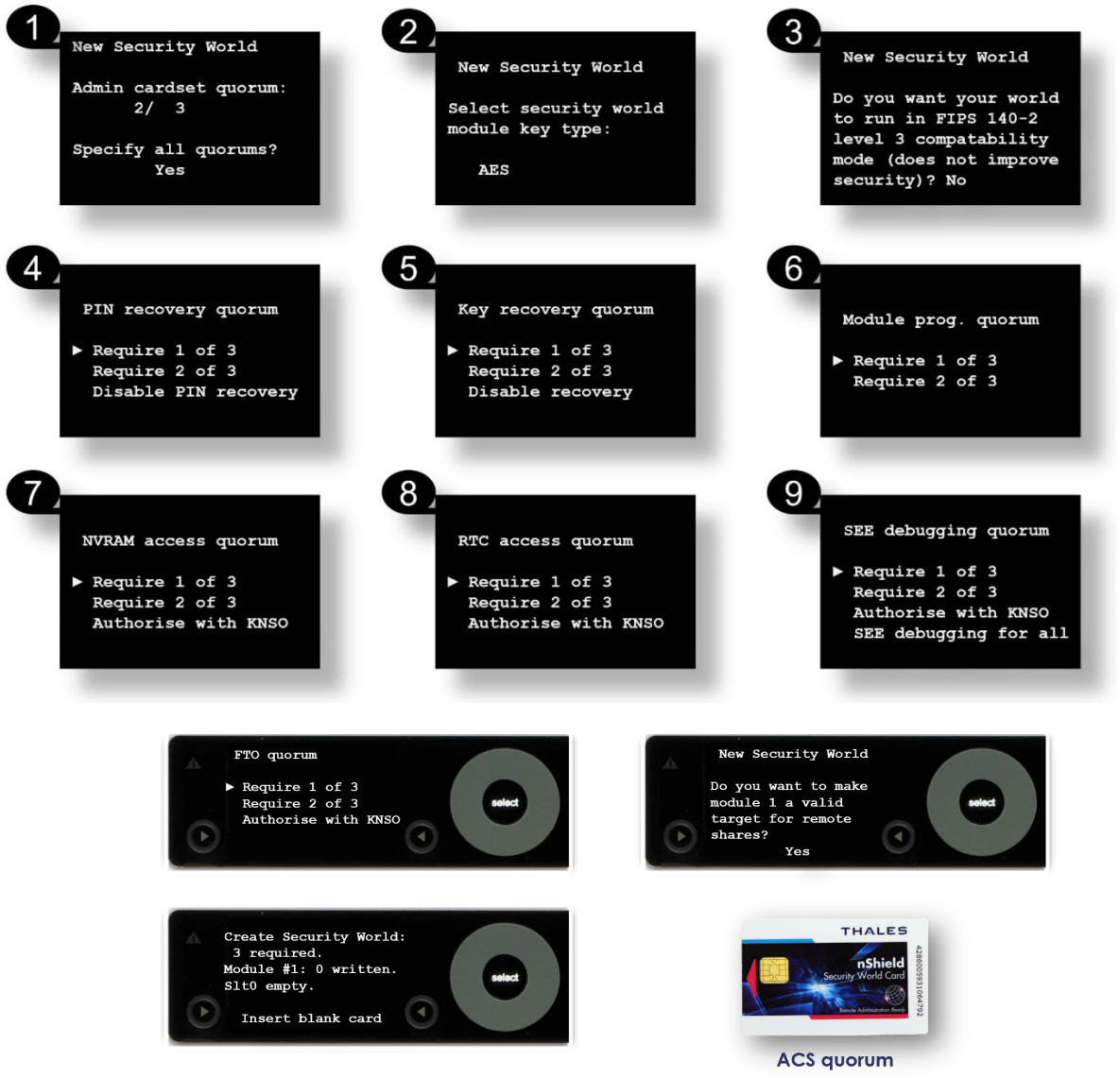
To create or load a Security World from Front panel

1. Create a new Security World (from menu 3-2-1)





Options for quorum



ACS quorum

Note: If you create a new Security World, you need a blank set of cards. If you load an existing Security World, you need an existing ACS.

2. Load a new Security World (from menu 3-2-1). Before a Security World can be loaded onto an nShield Connect you must ensure:
   - the nShield Connect is configured correctly with RFS
   - the RFS must have relevant Security World files in kmdata/local
   - A quorum of Administrator cards will be requested
   - Upon (re)loading Security World the option to configure with remote-share certificate is presented. (i.e) Use with Remote Operator.


3
System
HSM
▶ Security World mgmt
payShield
CodeSafe
select


3-2
Display World info
▶ Module initialization
RFS operations
Admin operations
Cardset operations
Card operations
select


New Security World
▶ Load Security World
Erase Security World
select


THALES
nShield
Security World Card
Remote Administration Ready
4286005931064792

ACS quorum

APPENDIX A

Install RFS Security World Software 12.60.7 on Linux

1. Extract files:

   - ***Change directory to " / "***
   - ***Un-tar the required components from CD:***

   - Step 1 : Extract "**SecWorld-linux64-user-12.60.7.ISO**" to folder say "SecWorld-linux64-user-12.60.7"

   - Step 2 : Go inside the extracted folder "SecWorld-linux64-user-12.60.07 " and you will the folder "**linux**" inside it. Transfer that folder to your Linux environment

   - Step 3 : Login to Linux environment and go inside amd64 folder and run " **find nfast -type f -name *.tar -print -exec tar -C / -xf {} \;**

   - ***Files are extracted to: /opt/nfast/***

2. Run the install script***:***

   - ***/opt/nfast/sbin/install***
   - ***Follow prompts until completed***
   - ***Reboot Machine***

Note: Refer to Appendix B for Security World Client Software Installation on Protegrity ESA Server.

APPENDIX B

Security World Client Software Installation on Protegrity ESA Server

1. Extract files:

   - ***Change directory to " / "***
   - ***Un-tar the required components from CD:***

   - Step 1 : Extract "**SecWorld-linux64-user-12.60.7.ISO**" to folder say "SecWorld-linux64-user-12.60.7"

   - Step 2 : Go inside the extracted folder "SecWorld-linux64-user-12.60.7 " and you will the folder "**linux**" inside it. Transfer that folder to your ESA environment

   - Step 3 : Login to ESA environment and go inside **linux\amd64** folder and run " **find nfast -type f -name *.tar -print -exec tar -C / -xf {} \;**

   - ***Files are extracted to: /opt/nfast/***

   - Step 4 : Copy KM-Data Local folder files from RFS Server to ESA Server at **/opt/nfast/kmdata/local** and Extract the contents of Security World Files, Module Files and Card Set files to "/opt/nfast/kmdata/local" path.

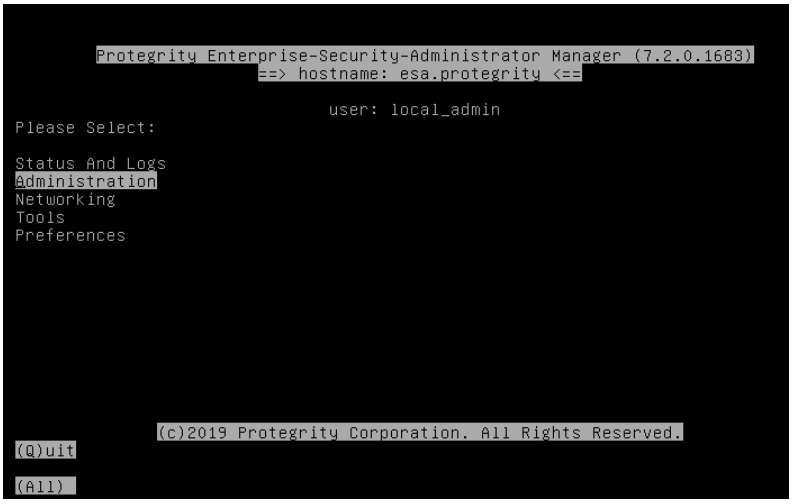
   - Step 5 : Set the permission for config file:
     chmod 775 /opt/nfast/kmdata/config/config

2. Stop LDAP Server on ESA:

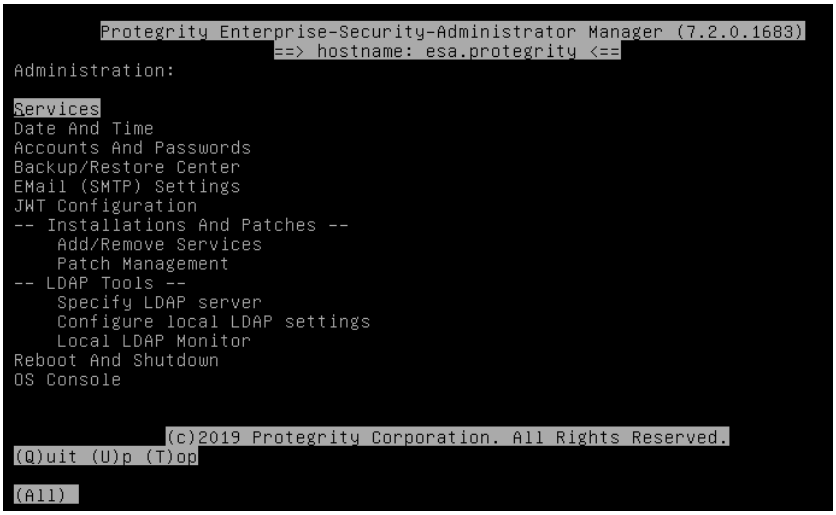
Step 1: Login to ESA CLI through "local_admin" account & "password"

-

Step 2: Go to Administration

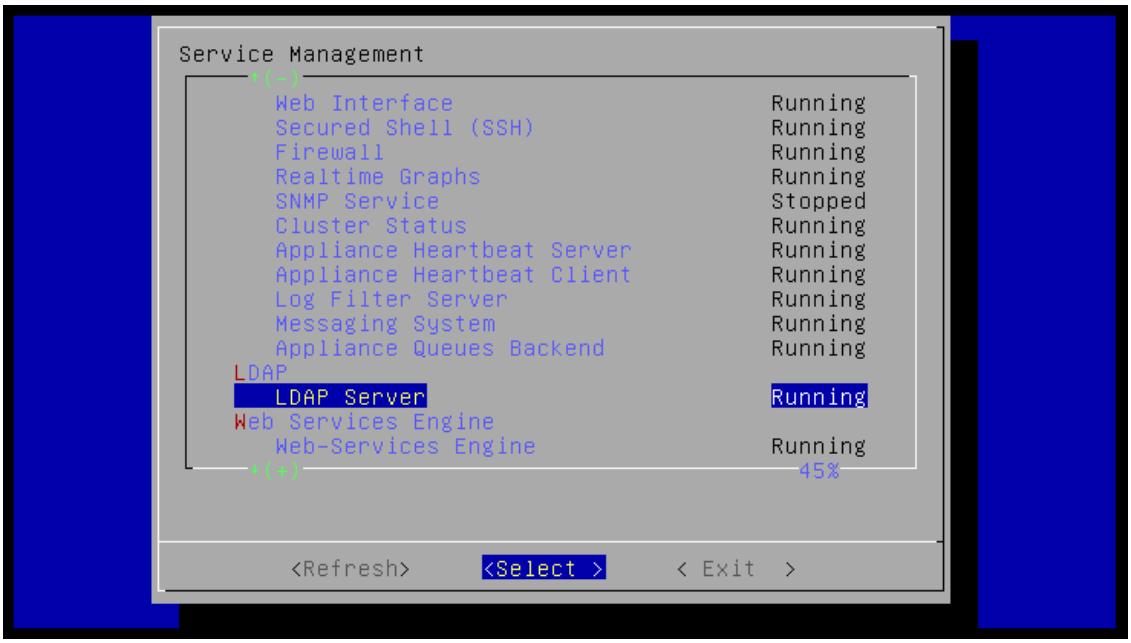


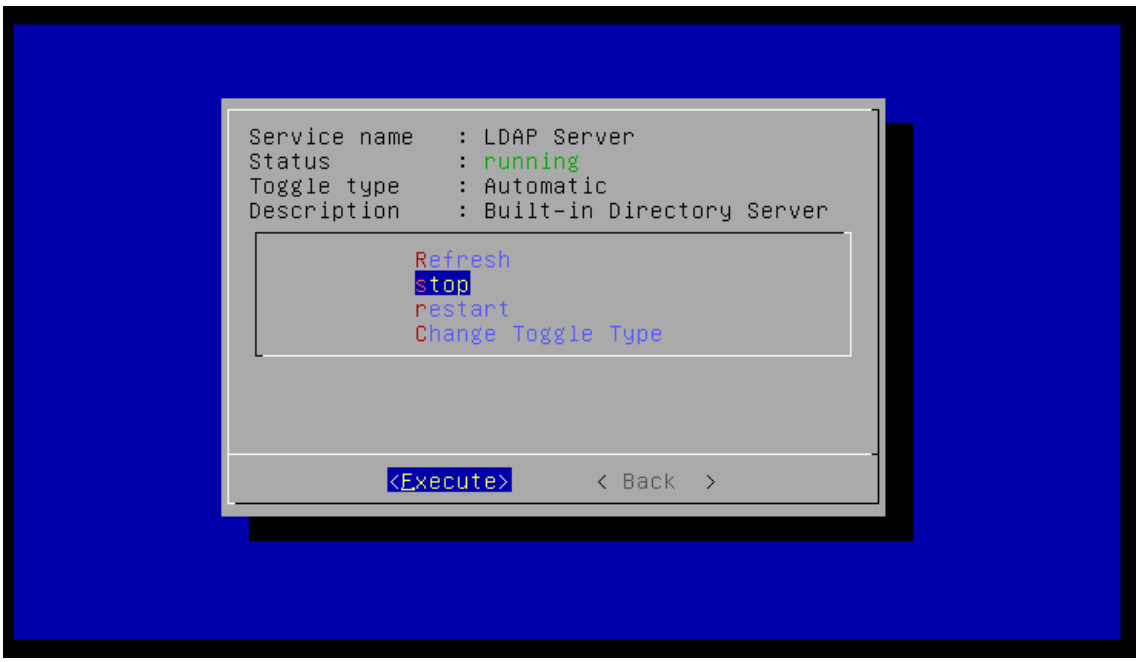
Step 3: Select Services



Step 4: In the Service Management Page

Select LDAP Server > Stop LDAP Server Services.

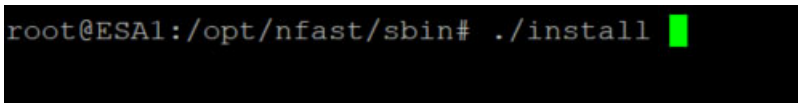




Note: LDAP server needs to be stopped as it conflicts with nfast user.

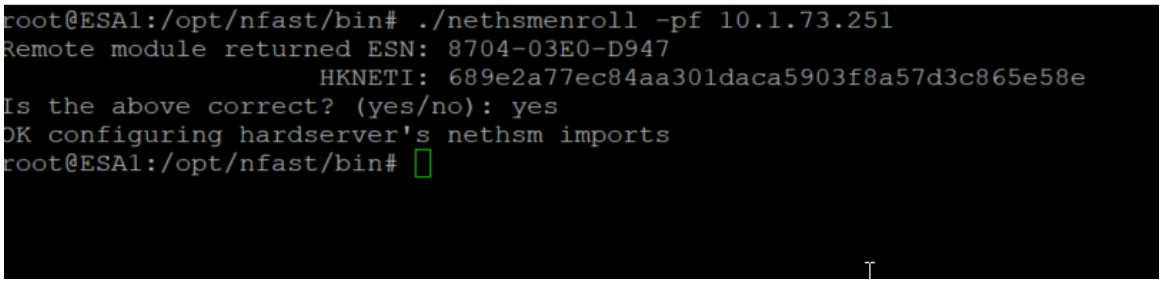
3. Install the Security World Client.

   - cd /opt/nfast/sbin
   - ./install



4. Query nShield Connect for ESN and HKNETI to verify during enrollment.
   - anonkneti -p 9004 <Ip-address of nShield(s)>

5. Enroll ESA as a client to HSM1 and HSM 2 using the command
   - ./nethsmenroll -pf <Ip-address of nShield> and repeat the step for second nShield as well



5. To verify nShield connectivity and security world health status, run **enquiry** and **nfkminfo** on ESA.

Note: The enquiry mode output of Module #1 and Module #2 should be **operational,** and the reply flags should be **none** before proceeding.

```
root@ESA1:/opt/nfast/bin# ./enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        8704-03E0-D947
 mode                 operational
 version              12.40.2
 speed index          478
 rec. queue           110..208
 level one flags      Hardware HasTokens
 version string       12.40.2+ main ddb26e9ca81bc44e9c2cbf5e336e693f9740f12f nsh
ield/nshield-project , 3.4pla2 Built on Apr 30 2018 11:22:00, Bootloader: 1.2.3,
 Security Processor: 2.1.18 , 12.45.2+ main 0ec1a5bcdb84d83f31724ebd33ecef471515
215c nshield/connect-project
 checked in           0000000059d623fa Thu Oct  5 07:22:18 2017
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
ollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp Ha
sLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds JobFragmentation LongJobsPr
eferred Type2Smartcard ServerHasCreateClient HasInitialiseUnitEx Type3Smartcard
HasKLF2
 module type code     0
 product name         nFast server
 device name
 EnquirySix version   4
 impath kx groups
 feature ctrl flags   none
 features enabled     none
 version serial       0
 remote server port   9004

Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        8704-03E0-D947
 mode                 operational
 version              3.4.2
 speed index          478
 rec. queue           22..50
 level one flags      Hardware HasTokens
 version string       3.4pla2 Built on Apr 30 2018 11:22:00, Bootloader: 1.2.3,
Security Processor: 2.1.18 , 12.45.2+ main 0ec1a5bcdb84d83f31724ebd33ecef4715152
15c nshield/connect-project
 checked in           000000005ae73497 Mon Apr 30 10:21:59 2018
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
```

6. In the output of ./nfkminfo the state should be usable in module sections

```
root@ESA1:/opt/nfast/bin# ./nfkminfo
World
 generation  2
 state       0x17a70000 Initialised Usable Recovery PINRecovery !ExistingClient RTC NVRAM FTO !AlwaysUseStrongPrimes !DisablePKCS1Padding !PpStrengthCheck SEEDebug
 n_modules   1
 hknso       d57c068fc73b6dc2a95fef3c7029349a0dd07abe
 hkm         8da1f78b99d514d5f7e0e1749d12d8e4c3683328 (type Rijndael)
 hkmwk       1d572201be533ebc89f30fdd8f3fac6ca3395bf0
 hkre        f236d665a9f671b129901b44b893b1741563ec87
 hkra        4e93aa6f9afb3951940e3974e669807658717a91
 hkmc        ff3433514b6ce8d09c6f608c988e9f3a5dcf2a09
 hkp         ff6204b42585e08e7cb6ac84b3f84b6b283b9c07
 hkrtc       baea53bd70b704a962a9cb99cf6a29d6ab35db31
 hknv        fc172c7b303ef7f9b18f9d3222497d715a1d9e0e
 hkdsee      3ed6d1cf103b8ccd94ec463b9c731822864b8816
 hkfto       1ebca96e50942684777e02c8fcc359ac28658bd4
 hkmnull     0100000000000000000000000000000000000000
 ex.client   none
 k-out-of-n  1/2
 other quora m=1 r=1 p=1 nv=1 rtc=1 dsee=1 fto=1
 createtime  2020-06-30 22:02:02
 nso timeout 10 min
 ciphersuite DLf1024s160mRijndael
 min pp      0 chars

Module #1
 generation 2
 state      0x2 Usable
 flags      0x10000 ShareTarget
 n_slots    2
 esn        8704-03E0-D947
 hkml       11bb209ab0eb9345a41002e27fe291c4e3cd4506

Module #1 Slot #0 IC 0
 generation    1
 phystype      SmartCard
 slotlistflags 0x2 SupportsAuthentication
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

Module #1 Slot #1 IC 0
 generation    1
 phystype      SoftToken
 slotlistflags 0x0
 state         0x2 Empty
 flags         0x0
```

7. Update Configuration Port.
   - vi /opt/nfast/kmdata/config/config
   - Search and replace nonprivy_port and priv_port.
   - nonpriv_port=8000 ###(default port is 9000)
   - priv_port=8001
8. Re-Start the nfast agent using
   - /opt/nfast/sbin/init.d-ncipher restart

Verify that nfast hardserver service should be running.

- /opt/nfast/bin/enquiry (Refer Step 5 as above)

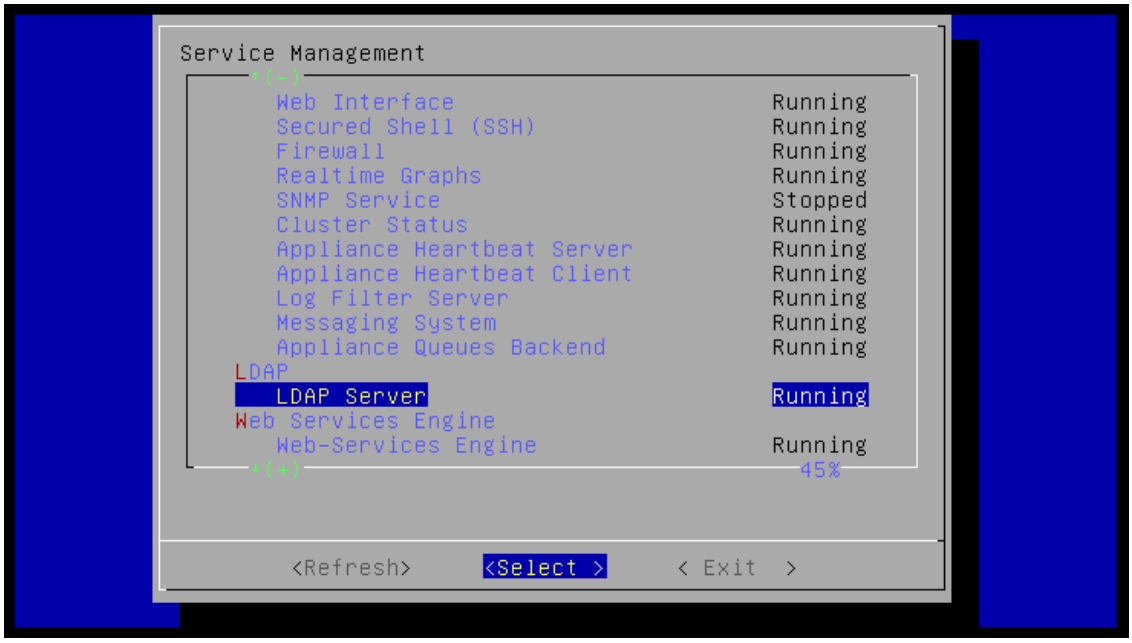
Verify that the PKCS 11

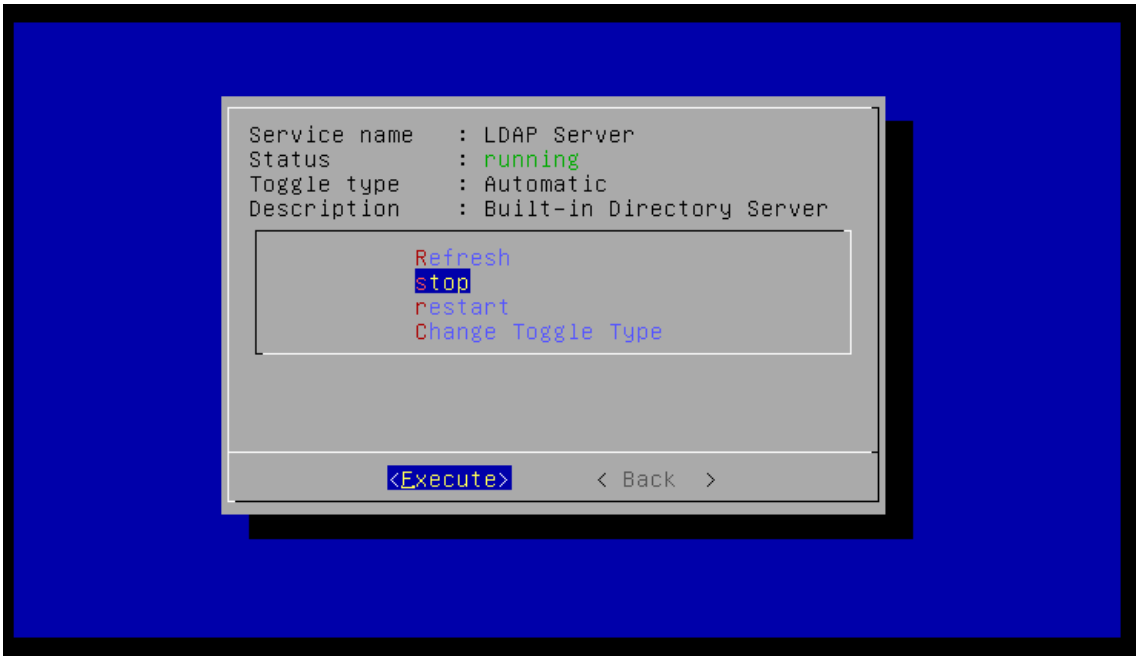
Verify it by running fine by running **"ckcheckinst"**

./ckcheckinst and select the OCS and supply with password.

```
root@ESA1:/opt/nfast/bin# ./ckcheckinst
PKCS#11 library interface version 2.01
                          flags 0
                 manufacturerID "nCipher Corp. Ltd                "
              libraryDescription "nCipher PKCS#11 12.40+          "
          implementation version 12.40

Slot  Status            Label
====  ======            =====
   0  Fixed token       "accelerator                     "
   1  Operator card     "ocs1                            "

Select slot number to run library test or 'R'etry or to 'E'xit: 1
Using slot number 1.

Please enter the passphrase for this token (No echo set).
Passphrase:

Test                      Pass/Failed
----                      -----------

1 Generate RSA key pair   Pass
2 Generate DSA key pair   Pass
3 Encryption/Decryption   Pass
4 Signing/Verification    Pass

Deleting test keys         ok

PKCS#11 library test successful.
root@ESA1:/opt/nfast/bin#
```

9. Start the LDAP server
    - Login to ESA CLI through “local_admin” account & “password” as stated in step 2 & start LDAP Server.





APPENDIX C

Switching to external nShield Connect

1. Add “service_admin” user to nCipher group, so that it can use nShield services.

   - usermod -aG nfast service_admin

   Reboot the ESA Server for the above command to take effect.

2. Login to Administrative OS Console to configure ESA HSM Gateway Service.

   a) Create a softlnk in the “/opt/protegrity/hsm/external” dirctory to the pkcs11 library.

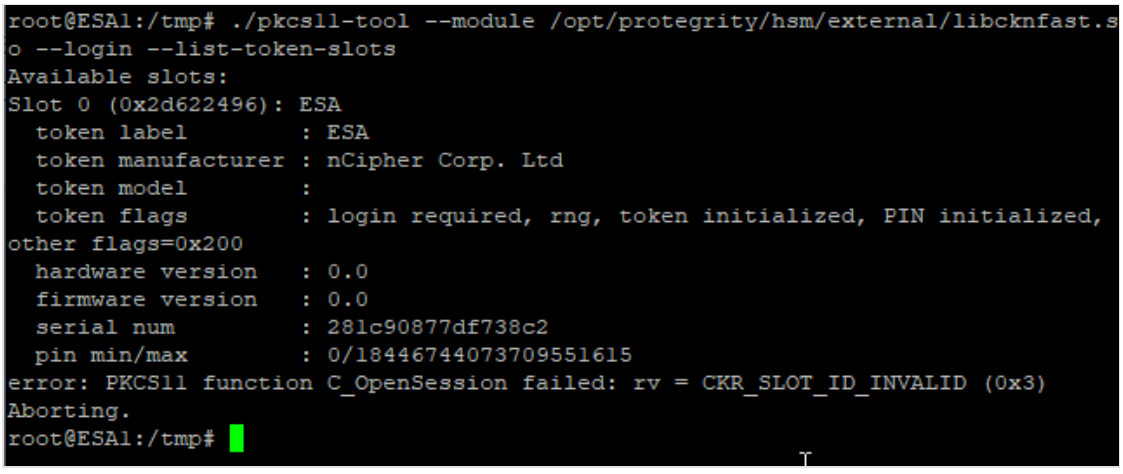
   ```
   sudo -u service_admin ln -s /opt/nfast/toolkits/pkcs11/libcknfast.so libcknfast.so
   ```

   b) Create a dummy configuration file.

   ```
   sudo -u service_admin touch /opt/protegrity/hsm/external/nfast.cfg
   ```

   c) Identify the nShield Connect Slot ID using pkcs11-tool

   ```
   pkcs11-tool --module /opt/protegrity/hsm/external/libcknfast.so --login --list-token-slots
   ```



   Depending upon the protection method used for key (ie. odule, OCS or Softcard), The above command will show all the token label & Slot ID in hex notation. One needs to convert the respective slot id hex value to decimal value which will be used in subsequent Protegrity HSM gateway configuration.

The Hex value 0x2d622496 corresponds to decimal value 761406614

d) Configure the external HSM environment variables.

Modify the entries in the “/opt/protegrity/hsm/external/hsm.env” file , set the respective values as below.

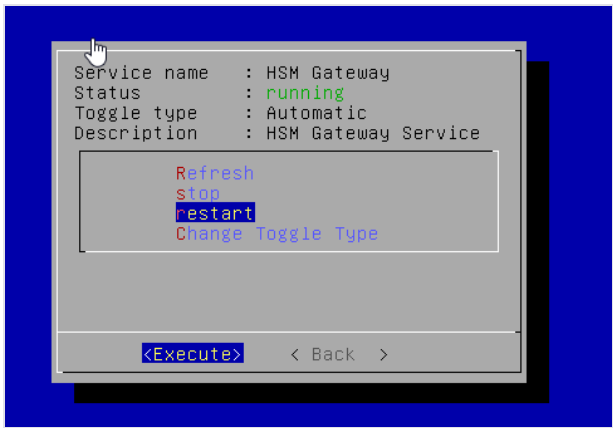
```
PTY_PKCS11_LIBRARY=${HSM_DIR}/libcknfast.so

PTY_PKCS11_ENV_KEY=NFAST

PTY_PKCS11_ENV_VALUE=${HSM_DIR}/nfast.cfg

PTY_PKCS11_SLOT= 761406614
```

Restart Protegrity’ HSM Gateway Services

First the HSM Gateway service need to be restarted to pick up the configuration changes made earler.

Login to the ESA’s local_admin cli (Refer Appendix-B , Step 2) Administration > Services > HSM Gateway.

Restart HSM Gateway Services.



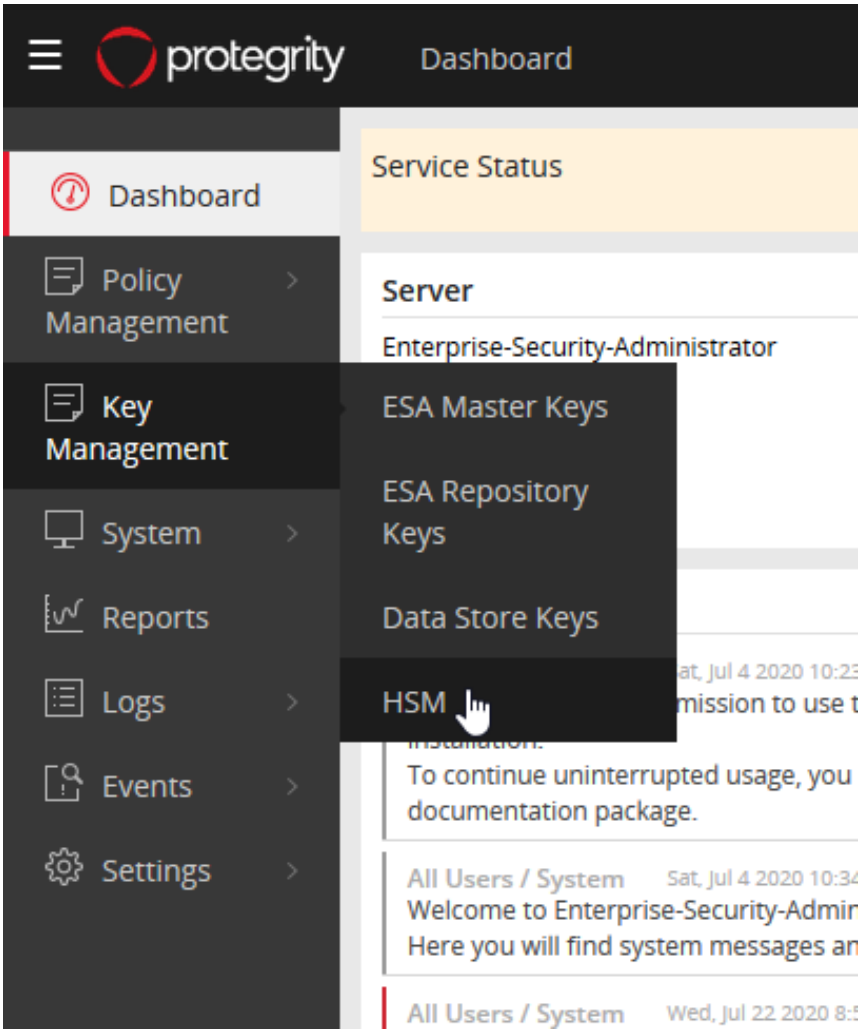
There shall be no errors in the `/opt/protegrity/p11gw/log/p11gwexternal.log` file. If there are errors one can increase the log level by setting `PTY_LOG_LEVEL=all` in the hsm.env.

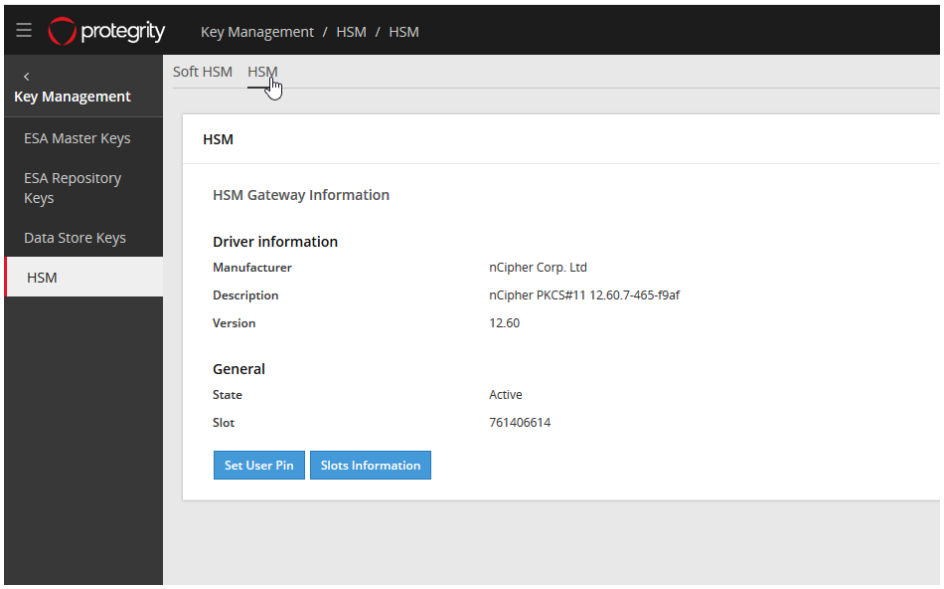
Make External HSM active (Switching From SoftHSM to HardHSM)

By default, ESA uses SoftHSM to store the Master Key. To set the nShield Connect as the active HSM, the pkcs#11 gateway services configured earlier requires the PKCS11 token user PIN to access protected pkcs#11 API's of nShield Connect. This is created from the ESA UI.

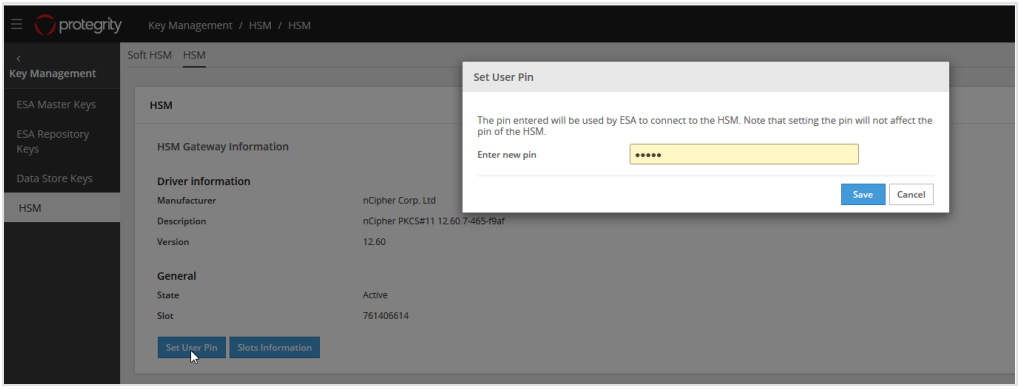
Login to ESA WEB UI using Admin privilege.

1. On the ESA Web UI, navigate to Key Management > HSM > HSM.

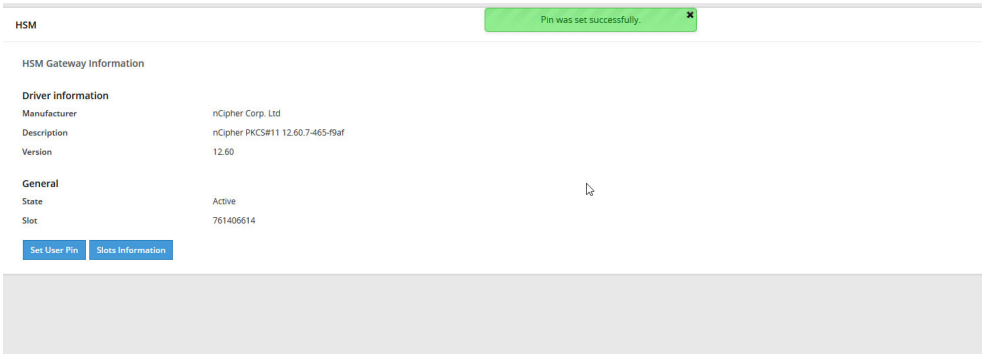




2. Click **Set User Pin**.

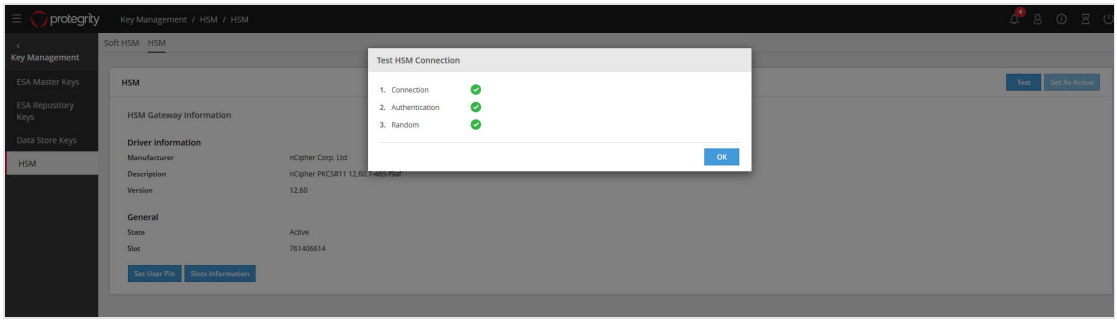


3. Enter the new PIN in the dialog and click **Save**



The ESA UI has built in functionality to verify the configuration. The test checks for connectivity and authentication to the HSM. It also validates if the HSM generates random bytes to determine successful authentication and connection.

1. Click **Test**.
2. The Test HSM Connection dialog box appears. If the test succeeds green icons shall appear for the tests performed.



3. Click **OK**.
4. Once the test is successful, we can now make nShield Connect the active HSM. Protegrity's pkcs#11 gateway services generates fresh Master key and re-encrypts all underlying keys like ERK or DataStore Keys from SoftHSM to HardHSM.
5. Click on Set as Active

This will ensure nShield Connect can access the Protegrity Master Key. One can also verify, a new key being generated under "/opt/nfast/kmdata/local".

It is utmost importance for client to back up the directory "/opt/nfast/kmdata/local". Refer relevant section for key backup and restore.

APPENDIX D

nShield High Availability of Master Key

Once a Master Key is created the key, world and module file must be made accessible to all nShield HSM's so that they may be part of the nShield estate.

To enable HA availability of the Master Key for all nShield's within the estate it is essential to perform the following.

Setup RFS :

1. Configure a client with the RFS for key management data exchange.

   rfs-setup.exe --gang-client --write-noauth <client_IP_address>

```
C:\Users\Administrator>rfs-setup --gang-client --write-noauth 192.168.42.241
Adding read-only remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\local exists
Adding new writable remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\local\sync-store exists
Saving the new config file and configuring the hardserver
Done
```

Perform on nShield Security World Clients:

2. Run on each client to exchange key management data with the RFS.

   rfs-sync --setup --no-authenticate <rfs IP address>

Key Management Steps on Client

3. Update key changes to the RFS

   rfs-sync --commit

4. Pull key data from RFS to local client

   rfs-sync --update

NOTE:
If a cooperating client has keys in its kmdata/local directory that are also on the remote file system, if these keys are deleted from the remote file system and then rfs-sync --update is run on the client, these keys remain on the client until they are rfs-setup manually removed.