Entrust Authority Security Manager 8.1 SP1

nShield® HSM nShield Integration Guide for Windows Server 2012 R2

Version: 1.8

Date: Friday, November 27, 2020

Contents

1   Introduction

1.1   This product

Entrust Authority Security Manager is a Public-Key Infrastructure (PKI) that manages digital certificates and can publish Certificate Revocation Lists (CRLs). The nCipher Hardware Security Modules (HSMs) are used to securely store and manage:

- The key pair for the Certificate Authority (CA).
- The key pair for the CRLs.

> Throughout this guide, the term HSM refers to nShield Solo/Solo+, nShield Connect/Connect+, and nShield Edge products.

1.1.1   Product configuration

The integration between the HSM and Entrust Authority Security Manager has been successfully tested in the following configurations:

Operating system	Entrust version	nShield Security World software version	nShield Solo/Solo+ support	nShield Connect/Connect+ support	nShield Edge support
Windows Server 2012 R2	8.1 SP1 with patch 192895	12.10 (hardserver 3.21.3)	Yes	Yes	Yes

nShield Solo/Solo+ firmware version	nShield Connect/Connect+ firmware version	nShield Edge frimware version
2.61.2	2.61.2	2.61.1

1.1.2   Supported nCipher functionality

Function	Supported
Key Generation	Yes
Key Management	Yes
Key Import	No
Key Recovery	Yes
1-of-N Operator Card Set	Yes
K-of-N Operator Card Set	Yes

Function	Supported
Softcards	Yes
Module-only Key	No
Strict FIPS Support	Yes
Load Balancing	Yes
Fail Over	Yes

> ℹ️ Fail Over and Load Balancing are not supported with the nShield Edge.

1.1.3   Requirements

To integrate the HSM and Entrust Authority Security Manager, you need the server and client machines to be set up as follows:

	Hardware	Software
Server	Windows Server 2012 R2 Datacenter	nShield Security World Software 12.10
		Openwave Directory Server 6.0
		PostgreSQL Server 8.3.23
		Entrust Authority Security Manager 8.1
Client	Windows Server 2012 R2 Datacenter	nShield Security World Software 12.10
		Security Manager Administration Console 8.1

Before attempting to install the software, we recommend that you familiarize yourself with the Entrust Authority Security Manager documentation and setup process and that you have the *User Guide* for your HSM available.

You also need to consider the following aspects of HSM administration:

- The number and quorum of Administrator Cards in the Administrator Card Set (ACS), and the policy for managing these cards.
- The number and quorum of Operator Cards in the OCS, and the policy for managing these cards.
- Key attributes such as the key size, persistence, and time-out.
- Whether there is any need for auditing key usage.
- Whether the Security World should be compliant with FIPS 140-2 level 3 and whether to use with the NIST SP800-131 suite of algorithms.

> ℹ️ The nShield Edge does not support NIST SP800-131.

1.1.4   Considerations

When installing the Openwave Directory Server (ODS) three separate passwords will be needed that are a minimum of 8 alphanumeric upper/lower case characters.

When installing PostgreSQL Server three separate passwords will be needed that are a minimum of 8 alphanumeric upper/lower case characters.

When initialising the CA five separate passwords will be needed that are a minimum of 10 alphanumeric upper/lower case characters.

When initialising the Directory System Agent (DSA) there are a number of attributes that must be considered before hand. These include items such as the name of the DSA, the administrator name and associated passwords, see "Configuring the DSA for use with your Entrust setup" on page 10 for a full list of required parameters.

> The passwords lengths given above are minimum password lengths. However, nCipher recommends you should use at least 12 characters (including alphanumeric and special characters).

1.2   This guide

This document explains how to set up and configure an Entrust PKI installation with an HSM. The instructions in this document have been thoroughly tested and provide a straightforward integration process. There may be other untested ways to achieve interoperability.

This guide may not cover every step in the process of setting up all the software. For more information about installing Entrust, see the Entrust documentation.

1.3   More information

For more information about the HSM, see the *User Guide* for the HSM.

Additional documentation produced to support your nCipher product is in the document directory of the CD-ROM or DVD-ROM for that product.

2 Procedures

To integrate Entrust Authority Security Manager and HSM:

> If you are using an nShield Edge, install the software first and then plug in the nShield Edge. If the nShield Edge is not reported or is reported as failed, open a command window as an Administrator, and navigate to **%nfast_home%\bin** and run **nc_hsc.exe**.

2.1 Summary

1. Install the HSM.
2. Install the nShield Security World Software, and configure the Security World.
3. Edit the **cknfastrc** file located in **C:\Program Files (x86)\nCipher\nfast\cknfastrc**.
4. Install and configure Openwave Directory Server 6.0:
    a. Install Openwave Directory Server 6.0.
    b. Configure the Directory System Agent (DSA) for use with your Entrust setup.
5. Install PostgreSQL Server 8.3.23.
6. Establish a preload session.
7. Install and configure Entrust Authority Security Manager 8.1 Service Pack 1 (SP1):
    a. Install Entrust Authority Security Manager 8.1 Service Pack 1 (SP1).
    b. Configure and initialize the Entrust CA.
    c. Initialize with K of N OCS (if using 1 of N see *Initializing the CA with 1-of-N OCS on page 26*).

All these procedures are described in the following sections.

2.2 Installing the HSM

Install the HSM using the instructions in the *Hardware Installation Guide* for the HSM. We recommend that you install the HSM before configuring the nShield Security World Software with your Entrust setup.

2.3 Installing the nShield Security World Software and creating the Security World

Install the nShield Security World Software and create the Security World as described in the *Hardware Installation Guide* for the HSM. This document assumes that:

- You are installing an offline root Certificate Authority.
- A new root key is generated during installation.

1. After creating the Security World, configure the cknfastrc environment variables. The **cknfastrc** file can be found in **C:\Program Files (x86)\nCipher\nfast\cknfastrc**. Edit the file to include:

```
CKNFAST_NO_UNWRAP=1

CKNFAST_NO_ACCELERATOR_SLOTS=1

CKNFAST_LOADSHARING=0  <see note below>

CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none NFAST_NFKM_TOKENSFILE=C:\Preload\<filename>
```

> The filename is user defined and will be referenced in the preload command. For example **%NFAST_HOME%\Bin>Preload -c** *<OCS Name>* **-f** *<pathname to preload file and filename>*.

> When using a K-of-N cardset where K>1, set **CKNFAST_LOADSHARING=0**. When using a K-of-N cardset where K=1, set **CKNFAST_LOADSHARING=1**.

> For more information about the environment variables used in **cknfastrc**, see the *nShield PKCS #11 library environment variables* section in the *User Guide* for the HSM.

> For Enhanced Database Protection (EDP) use **CKNFAST_LOADSHARING=0** after enabling the database hardware protection. Restart the system for load sharing to work.

2.4   Installing and configuring Openwave Directory Server 6.0

This section describes how to:

- Install Openwave Directory Server 6.0.
- Configure the DSA for use with your Entrust setup.

2.4.1 Installing Openwave Directory Server 6.0

Openwave Directory Server is based on X.500 recommendations and LDAPv3 standards; your Entrust setup uses it to store the user profiles that the Entrust Administrator creates.

To install Openwave Directory Server 6.0:

1. Obtain the Openwave Directory Server software and run **setup.exe**.
2. Accept the license agreement, select a complete installation and follow the install wizard through to completion.

2.4.2   Configuring the DSA for use with your Entrust setup

You should consider the DSA you are initializing, in the example below DSA1 is indicative of a primary DSA, for further information refer to the Openwave documentation.

To configure the DSA for use with your Entrust setup:

1. Right click on the command prompt and select **Run as Administrator**.

2. Run commands of the following form (which shows the example DSA created with Openwave Directory Server):

```
cd C:\ C:\>md DSADATA\DSA1

C:\>cd DSADATA\DSA1

C:\DSADATA\DSA1>odsecreate.cmd
```

This will create a DSA in the current working directory.

5. Follow the process described in the following table to configure the DSA for use with the Entrust CA. Use nomenclature appropriate for your DSA, the table below is given as an example:

Text on screen:	You enter:
Please enter the name of the DSA	cn=<name of DSA>
Please enter the name of the DSA administrator	cn=<DSA administrator name e.g. diradmin>
Please enter the administrator's password	*<Administrator's password>*
Please enter the port number for DAP/DSP	1001
Please enter the port numer for shadowing. Press return for no shadowing, this can be added later	2200
Please enter the port number for LDAP. Press return for no LDAP, this can be added later	389
Please enter the license key	*<license key>*
Do you wish to include the extensibleObject defined in RFC 2252 (Y/N)?	N
Do you wish to include the Java(tm) Objects schema defined in RFC 2713 (Y/N)?	N
Do you wish to include the CORBA Objects schema defined in RFC 2714 (Y/N)?	N
Do you wish to include the LDAP as a NIS Schema defined in RFC 2307 (Y/N)?	N

Text on screen:	You enter:
Do you wish to include the UPS Common schema defined by Openwave messaging (Y/N)?	N
Do you wish to include the ACP133 schema defined by Openwave messaging (Y/N)?	N
Initializing the DSA	
Reading country codes from file iso3166 admin>Reading country codes from file iso3166 admin>Log file was odscreate.000	
Please enter 'Y' to configure an empty Entrust DSA or 'N' to add the CA, Search Base (CP) and Entrust Directory Manager entries	N
Please enter the name of the search base in the DSA It must be either a country, organization, organizational unit, domain or locality	o=CAname <enter appropriate CA name>
Please enter the name of the CA in the DSA. It must be either a country, organization, organizational unit, domain, locality, organizational role, application processor or device. Press return for top entry to be the CA	CA = o=CAname
Please enter the CA's password	*<CA's password>*
Please enter the name of the Entrust Directory Manager	cn=manager
Please enter the Entrust Directory Manager's password	*<Directory Manager's password>*
Initializing the Entrust DSA Changing update log	
Openwave Messaging Directory Server Demo18 June 2017	
Reading country codes from file iso3166 admin>admin>Log file was odsecreate.000 Do you wish to start the DSA (Y/N)?	Y
Starting the DSA Creating the file 'ds.properties' Writing ldap/attributes.cfg	

Text on screen:	You enter:
Writing ldap/objectclasses.cfg	
Writing ldap/syntaxes.cfg	
Writing ldap/matchingrules.cfg	
Writing ldap/oidtable.at	
Writing ldap/oidtable.oc	
Writing oidslocal	
odssched<process ID> started	

This command can either be minimized or closed if desired once the DSA has successfully started. If the ODS is not started, run the command **odsstart** and to stop the ODS run the command **odsstop**.

2.5   Installing PostgreSQL Server 8.3.23

To install PostgreSQL Server on the server machine:

1. Download PostgreSQL Server installer from the Entrust TrustedCare online support site for the Windows operating system (SM_81_Win_Postgre SQL_8323_setup.exe).

2. To start installing the PostgreSQL database for Entrust Security Manager 8.1 SP1, double-click the setup file SM_81_Win_Postgre SQL_8323_setup.exe.

3. Accept the license agreement for the installation.

4. Accept the default destination folder (C:\Program Files (x86)\Entrust) for installing the Entrust PostgreSQL Database program files, and then click Next.

5. In the Select Drive for Database window, accept the default location as drive C:\, and then click Next.

6. In the Database Transaction Log Drive window, select the drive that will host database logs, then click on Next. The default path is C:\.

7. In the Possible Data Security Issue dialog box which states:

```
For Security of your data, we recommend that the Transaction log should be stored in
a separate partition. Would you like to change your selection?
```

9. Select No (transaction logs can be set to a different partition on the same server, if required).

10. In the PostgreSQL Windows Account Password window, set the password for **easm_entrust_pg** account, and then click Next.

11. In the Password for Database User window, provide the password for the account **easm_entrust** and click on Next. See the Entrust password criteria for guidelines on setting the password. If the password is weak, the wizard gives a message asking to change the password.

    Press Yes to reset the password, otherwise press No to continue with the set password.

13. In the Password for Database Backup user window, set the password for **easm_entbackup** account. To continue, click Next.

14. In the PostgreSQLDatabasePort window, accept the default port 5432. To continue, click Next.

15. In the Check Setup Information window, verify the paths of Program files, Database, Transaction logs, and port details. To continue with the installation, click Next.

16. To complete the installation, click Finish in the InstallShield Wizard Complete window.

> ⓘ Before installing Entrust Authority Security Manager, you must preload the OCS cardset being used to protect the Entrust keys.

2.5.1 Using preload with a K-of-N OCS

To initialize the Entrust Authority Security Manager with a K-of-N OCS:

1. Create an empty folder called **Preload** on drive **C:**.

2. Right click on a command prompt and select **Run as Administrator** and navigate to **C:\Program Files (x86)\nCipher\nfast\bin>**.

3. Run the following command to list the OCS:

   ```
   nfkminfo.exe -c
   ```

5. Preload the cardset by running the following command:

   ```
   preload -c <cardsetname> -f <pathname>\<filename> pause
   ```

   The filename is user defined but must be consistent when setting the variable in cknfastrc and invoking preload. For example:
   A variable set in cknfastrc: **NFAST_NFKM_TOKENSFILE=C:\Preload\filename**
   A variable invoked with preload: **>preload.exe -c ocsname -f "C:\Preload\filename" pause**

8. Present the OCS when prompted and enter the passwords for the OCS.

   You must keep the preload command window active. You can minimize it but **do not close** it, otherwise you will shut down the session. You can confirm that the cardset has preloaded by opening another command window and running the

command below. The loaded Objects will be reported.

```
preload.exe -c <cardsetname> -f C:\preload\<filename> nfkminfo
```

Useful information concerning Operator Card Sets (OCS):

- You must present sufficient different OCS cards to fulfil the quorum. (The passphrase (if any) can be different for each OCS card).

- If non-persistent cards are used, then the last card in the quorum must remain inserted in the card reader.

- If persistent cards are used, then the last card in the quorum can be removed from the card reader.

- The tokens file is generated by the preload utility and is valid for one continuous session only. If the session is lost then the token authorization is lost. You cannot reuse the same token file once the session is lost, even if you will use the exact same OCS cards again. To restart, you must delete the expired tokens file, and will have to go through the entire preload sequence again.

- A session, and tokens authorization may be lost if:
  - There is a temporary power failure
  - You remove the last card in the quorum if they are non-persistent OCS cards
  - You clear the module.

> ⚠️ The tokens file represents a security risk if permissions to access it are not restricted to authorized persons only.

2.6   Installing and configuring Entrust Authority Security Manager 8.1 SP1

2.6.1   Installing Entrust Authority Security Manager

To install Entrust Authority Security Manager on the server computer:

1. Download Entrust Authority Security Manager 8.1 Service Pack 1 (SP1) from the Entrust TrustedCare online support site for the Windows operating system (SM_81_Win_setup.exe).

2. Run the installation program and accept the default installation path (C:\Program Files (x86)\Entrust).

3. A command prompt will appear requesting the password for user easm_entrust: enter the password and press enter to proceed with the installation. The same password for user easm_entrust: is used when installing the Postgres.

4. When the installation process is complete, select the option to run the Entrust Configuration Utility, and then click Finish.

2.6.2 Configuring the Entrust CA

To configure the Entrust CA:

1. After the installation, the Entrust Authority Security Manager Configuration setup screen appears. If it does not appear, select Start > Entrust > Security Manager Configuration.

2. In Select the configuration type, select Custom configuration, and then click Next.

3. When prompted, enter the Enterprise licensing information that appears on your Entrust licensing card:

   - Serial Number

   - Enterprise user limit

   - Enterprise licensing code.

4. Accept the default installation paths for the data files (c:\authdata) and backup files (c:\entbackup).

5. Select the LDAP directory. Enter the directory node name (*Server name* or IP address) and directory listen port (389).

6. When prompted for the CA DN and password, enter the information you provided when configuring the DSA for use with the Entrust set up (see "Installing and configuring Entrust Authority Security Manager 8.1 SP1" on the previous page) and click on **Test Bind Information**. If this does not result in a **Bind Successful** response, ensure that server name or IP address are correct and that the DSA is running and rebind the information:

CA DN	o=CA<name>
CA Directory access password	*<password>*

7. Enter the information for the Directory Administrator and test the bind before committing it by clicking **Next**:

CA DN	cn=<manager>
Directory access password	*<password>*

8. In the **Advanced Directory Attributes** dialogue, verify the information for the First Officer, and then click Next:

CA DN	cn=First Officer, o=CA<name>

9. Make sure **Verify Directory information now** is checked, then click Next to got to the Verify Directory Information now page.

10. Use the Entrust Directory Verification Tool (EntDVT) to verify the settings, and then click Next.

At the bottom of the dialogue there should be no errors in the Summary section:

```
Summary: Total number of fatal errors: 0 Total number of errors: 0 Total number of
notes: 0
```

12. When prompted, provide your Windows login credentials, and then click Next.

13. Select EASM_Entrust_PostgreSQL for database connection and leave the **Enable autologin for automatic service startup** unchecked.

14. Enter the password that was assigned to **easm_entrust** when you installed the PostgreSQL Server 8.3.23, see "Installing and configuring Entrust Authority Security Manager 8.1 SP1" on page 14, and then click Next.

15. Enter the password that was assigned to the backup user when you installed the PostgreSQL Server 8.3.23, see "Installing and configuring Entrust Authority Security Manager 8.1 SP1" on page 14, and then click Next.

16. When asked whether to:

```
InterOperate with Microsoft (TM) CryptoAPI-enable applications?
```

Select No and click Next.

19. Configure the following settings as appropriate, and then click Next:

Security Manager node name	*<Server machine>*
Security Manager listen port	709
Administration subsystem listen port	710
PKIX-CMP subsystem server port	829
Entrust XML administration protocol port	443
Enable XAP subsystem	Checked

20. In the Cryptographic Information dialog, select settings as appropriate, for example:

Certificate Authority	
CA key generation	Hardware
CA Key Type	RSA2048*
Database	
Database Encryption Algorithm	AES-CBC-256

Entrust Users	
User Signing Key Type	RSA2048
User Encryption Key Type	RSA2048
CA Signing Algorithm	
Signature algorithm	RSA-SHA256
Policy Certificate	
Policy certificate lifetime (in days)	30

*Consult your security policy document for the recommended key sizes and algorithms to use.

> In order for this integration to work with EC-P and RSAPSS the nShield HSM must have ECC activation feature enabled (in **%NFAST_HOME%\bin** directory run **FET.exe**).

21. Click Next.

    The system returns the following message:

    ```
    Security Manager Configuration could not detect any hardware devices. Please select
    a new cryptographic hardware library in the next dialog
    ```

24. Click OK.

25. Use the nShield PKCS11 library located at **C:\Program Files (x86)\nCipher\nfast\toolkits\pkcs11\cknfast.dll**.

    You can confirm this location by opening the **entmgr.ini** file located in the **Entrust** directory and looking for the entry: **CryptokiV2LibraryNT = C:\Program Files (x86)\nCipher\nfast\toolkits\pkcs11\cknfast.dll**.

27. Select the appropriate slot for the desired type of protection.

28. If you require the CA to issue and revoke certificates beyond the year 2037, select **No** and click **Next**.

29. When prompted, select Root CA to create a Root Certificate Authority.

30. When prompted to initialize the CA certificate, approve the initialization, and then enter the following certificate properties:

CA cert lifetime	120 months*
CA private key usage period	100%

*Consult your security policy document for CA lifetime.

31. If you want to continue to initialize the CA select the check box **Run Security Manager Control Command Shell now** and click **OK** to be taken to the first time initialization **entsh** command shell and enter passphrases when prompted, otherwise deselect the checkbox and select **OK**. You will have the option to initialize the CA later by running the init command from the **entsh** command window.

> You will be prompted to enter 5 passphrases, these should be different and known only to the individuals concerned. When setting passwords for Master users (x3), First Officer and **CA Hardware** note the following constraints:
>
> - The password must be at least 10 characters in length and not based on a dictionary word.
> - The characters must be both a mix of upper and lower case and include numbers.

> If you choose to protect your root CA private key with a 1-of-N OCS see *Initializing the CA with 1-of-N OCS* on page 26.

32. Verify the CA key is loaded into the hardware by opening an entsh$ and running the command:

```
ca key show-cache
```

34. Check the hardware status:

```
hardware status: Loaded >> 'nCipher Corp. Ltd SN : XXXXXXXXXXXXX SLOT : XXXXXXXX'
```

2.6.3   Backup

You must ensure that the Security World \local directory (C:\ProgramData\nCipher\Key Management Data\local) is backed up after any new key generation or Security World administration activities have occurred and that the backups are stored appropriately in case a disaster recovery scenario needs to be invoked.

2.6.4   Restore Entrust to a new server when using an nShield HSM

In order to execute a full restore of the Entrust environment when using an HSM you must ensure that you have the backed up data from the nShield Security World /local directory and the Entrust Security Manager backup (mgrbkYYYYMMDDHHMMSS).

2.6.5   Procedure overview

1. Install the new Windows server, this should be the same operating system as the original including the version and patching level.

> It is recommended that you use the same host name and IP address that you used on the original computer. You can change the host name or IP address, but you must change all references to the host name or IP address in the **entrust.ini** and **entmgr.ini** files. Additionally, ensure that you use the same user accounts, groups, and directories when installing PostgreSQL and Security Manager.

2. Install the HSM and nShield Security World software. You will need to have access to the Administrator Card Set (ACS) and the Operator Card Set (OCS) quorums and associated passphrases.

3. Install and configuring Openwave Directory Server 6.0.

4. Install PostgreSQL on the new server. Use the same directories, drives, passwords, and ports that you used on the original server.

5. Verify Security World condition and load Security World if necessary.

6. Edit the cknfastrc file located in C:\Program Files (x86)\nCipher\nfast\cknfastrc, see *Installing the nShield Security World Software and creating the Security World* on page 8.

7. Ensure that the kmdata/local directory contains the correct Security World data.

8. Run the preload command.

9. Install Security Manager. Use the same paths and drives that you used on the original server.

2.6.6 Application software installation on the new server

To recover your Entrust installation to a new server when using an nShield HSM:

1. Install the new Windows server. When installing the new server, ensure that it is identical to the old server (same operating system, including versions and patches).

   It is recommended that you use the same host name and IP address that you used on the original computer. You can change the host name or IP address, but you must change all references to the host name or IP address in the entrust.ini and entmgr.ini files. Additionally, ensure that you use the same user accounts, groups, and directories when installing PostgreSQL and Security Manager.

3. Install the HSM and the Security World software on the new host server. For details on installing and configuring Security World and nShield HSMs refer to the user guides which can be found on the Security World release software DVD.

4. Install Openwave Directory services on the new server.

   Initialize the DSA with the same settings as on the original server.

6. Install PostgreSQL on the new server.

   Use the same directories, drives, passwords, and ports that you used on the original server.
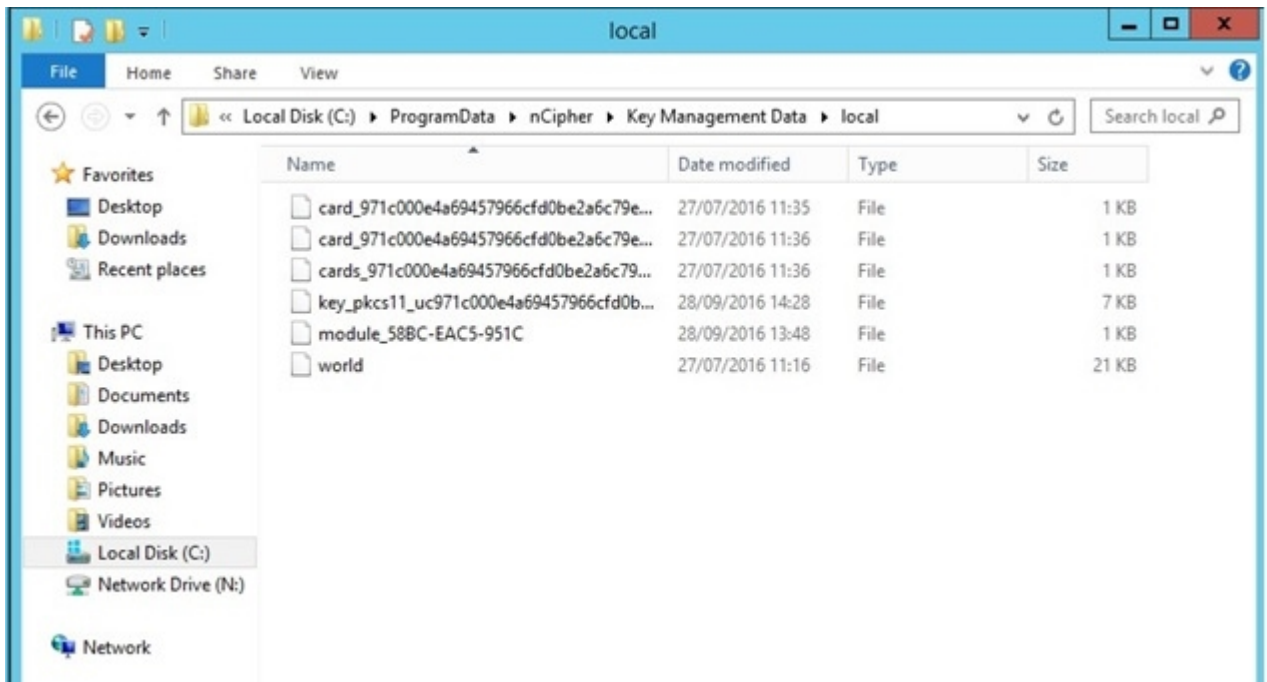
8. Confirm that the HSM is correctly installed by running the enquiry command The HSM will usually be reported as Module #1(unless you are using multiple HSMs) the Module # mode should be reported as operational:

```
C:\Program Files (x86)\nCipher\nfast\bin>enquiry.exe Server: enquiry reply flags
none enquiry reply level Six serial number 2958-B193-14D7 mode operational Module
#1: enquiry reply flags none enquiry reply level Six serial number 2958-B193-14D7
mode operational
```

10. From the backed up \local directory, copy and paste the contents into the new \local directory:

```
C:\ProgramData\nCipher\Key Management Data\local
```

Ensure that the HSM Electronic Serial Number (ESN) module xxxx-xxxx-xxxx matches that reported in the enquiry output. Below is an example of *\local* directory contents showing Operator cards Hashes, module ESN and world file:

14. Confirm that the Security World is running correctly by running the nfkminfo command.

```
C:\Program Files (x86)\nCipher\nfast\bin>nfkminfo.exe
```

If there is an exclamation mark ! immediately before Usable, then check under Module for reported condition.

```
C:\Program Files (x86)\nCipher\nfast\bin>nfkminfo.exe World generation 2 state
0x37b50000 Initialised !Usable Recovery PINRecovery !ExistingClient RTC NVRAM FTO
AlwaysUseStrongPrimes !DisablePKCS1Padding !PpStrengthCheck SEEDebug StrictFIPS140
```

The error condition is reported via the module **state**. If **unchecked** is reported as **state** then you should re-load the Security World onto the HSM.

```
Module #1 generation 2 state 0x9 Unchecked flags 0x0 !ShareTarget n_slots 2 esn
5964-C7A0-6AA8
```

20. To load the Security World onto the module, place the HSM into **Initialisation** mode and run the new-world command; **new-world –l –m#** (where # is the reported module number e.g. module #1.

```
C:\Program Files (x86)\nCipher\nfast\bin>new-world –l -m1
```

Once the world has been loaded onto the HSM, put the HSM back into **Operational** mode and confirm that the Security World is available and usable by running **nfkminfo**, again; the exclamation mark should no longer be visible.

> If state is reported as **Foreign**, this is indicative of a mismatch of the world file, i.e. the world file in the \local directory is incongruous to the Security World loaded onto the HSM. Ensure that you are using the correct back up if you are utilising multiple Security Worlds in your environment (if in doubt contact nCipher Support.

23. Open a text editor and add the below to the **cknfastrc** file in **C:\Program Files (x86)\nCipher\nfast\cknfastrc**:

```
CKNFAST_NO_UNWRAP=1 CKNFAST_NO_ACCELERATOR_SLOTS=1 CKNFAST_LOADSHARING=0 CKNFAST_
OVERRIDE_SECURITY_ASSURANCES=none NFAST_NFKM_TOKENSFILE=C:\Preload\<preload_
filename>
```

> **NFAST_NFKM_TOKENSFILE=C:\Preload\<filename>** the **<filename>** must be the same as on the original server. This will be named in step 5 when the **preload** command is run. Once the above edits have been made save the file and close the editor. Details can be found in *Installing the nShield Security World Software and creating the Security World* on page 8.

25. Ensure that all expected keys are present by running **nfkminfo.exe –k**, this will report all keys available to the Security World there should be at least **1** key reported:

```
C:\Program Files (x86)\nCipher\nfast\bin>nfkminfo.exe -k
```

27. Run the nShield preload session. Open a command window, right click and select **Run as Administrator**, navigate to the *%NFAST_HOME%\bin* directory and run the preload command:

```
C:\Windows\system32>cd %nfast_home%\bin C:\Program Files
(x86)\nCipher\nfast\bin>preload.exe -c OCS_name -f C:\path_to_preload_file\preload_
filename pause
```

Present the quorum of Operator Cards and enter the passphrase when prompted to do so. Do not close the command window, as this will terminate the preload session.

30. Install the same version of Security Manager that you used on the old server. Use the same paths and drives that you used on the original server. For further details refer to the document SM_81SP1_Operations_issue16.

> **i**   Do not configure or initialize Security Manager.

Continue to recover the environment as per the detailed description in the Entrust Operation document SM_81SP1_Operations_issue16 in the section **Restoring data to a new server from a backup**. See notes below.

2.6.6.1 Notes on the SM_81SP1_Operations document:

2.6.6.1.1 Step #9 - Where you are advised to:

*"Copy the Security Manager backup (**mgrbkYYYYMMDDHHMMSS**) from the original server to the new server. It is recommended that you copy the backup into the entbackup folder on the new server."*

You will need to manually create a folder called entbackup to copy the mgrbkYYYYMMDDHHMMSS folder to as this does not exist at this stage.

2.6.6.1.2 Step #12 Subsection b and c

"Set the database password in the dbloginpw= setting" and *"Set the database backup password in the dbBackupPw= setting"*

Be aware that dbloginpw and dbBackupPw do not exist in the login section, enter these in full together with the actual passwords for these two roles, i.e.

```
C[login] maxProcs=256 .. .. dbloginpw=Password dbBackupPw=Password
```

Save the file and exit.

2.6.6.1.3 Step #12 Subsection f and g

"Remove the encrypted dbloginpw setting" and *"Remove the encrypted dbBackupPw setting"*.

Only delete the data , you should not delete the headings themselves, example of the authauto.ini file after dbloginpw and dbBackupPw credentials removed:

```
[dbloginpw Credentials] [Hardware Info]
CAKey=6E43697068657220436F72702E204C74642020534E203A20393731633030306534 _continue_
=61363934353739 DbProt=2020534E203A20
HwList=6E43697068657220436F72702E204C74642020534E203A2039373163303030653 _continue_
=461363934353739X [dbBackupPw CredentialsC[login]
```

12. Verify the restore process by logging in to entsh and running:

```
entsh$ login Master User Name: Master1 Password: You are logged in to Security Manager
Control Command Shell. o=nCipher.Master1 $ ca key show-cahw -type all EAC is not enabled.
There is no associated cryptographic hardware for EAC.[dbloginpw Credentials]. ****
Hardware Information **** ------------------------------------------------- Name:
nCipher Corp. Ltd SN : 971c000e4a694579 SLOT : 492971158 Has current X.509 CA key: Y Load
Status: hardware loaded ok Uses Password: Y DB protection HW: N In use for X.509 CA keys:
Y In use for EAC keys: N ------------------------------------------------- **** End of
Hardware Information **** o=nCipher.Master1 $ ----------------------------------------
--------
```

The HSM name/serial number (SN :) should be displayed and **hardware loaded ok** should
be reported.

3   Troubleshooting

The following table lists error messages that might be displayed during the procedures described in this guide.

Problem	Cause	Resolution
(-8973) Could not connect to the Entrust Authority Security Manager service. Security Manager service may not be running.	The Entrust service is not running in the Entrust Authority Master Control shell (entsh$).	Open the Master Control shell (entsh$): 1. Login with Master1. 2. Run Service Start.
(-2229) An error occurred. Check the service status and manager logs for details.	Timeout issue.	Login to entsh and run service status, if the service is shown as down start the service with service start.

Appendix A Installing Entrust Authority Security Manager 8.1 Service Pack 1 (SP1)

The following steps detail how to install Entrust Authority Security Manager 8.1 Service Pack 1 (SP1) on older versions of Windows Server (i.e Windows Server 2008 R2, installing Entrust Authority Security Manager 8.1 Service Pack 1 (SP1) on older versions is not supported).

To install the Entrust Authority Security Manager 8.1 Service Pack 1:

1. Close all open applications to prevent conflicts from open applications that use shared files during the upgrade.

2. Ensure that your Security Manager database and LDAP-compliant directory are running.

3. Download the upgrade installer (SM_81SP1_Win_upgrade.exe) from Entrust TrustedCare (https://secure.entrust.com/trustedcare).

4. Run the upgrade installer (SM_81SP1_Win_upgrade.exe) to start the upgrade. The InstallShield Wizard appears. Follow the Wizard to begin the upgrade.

5. A Security Manager Control Command Shell window appears. When prompted, enter the password for easm_entrust.

6. When prompted, enter your Master User name and password.

7. Press Enter to close the Security Manager Control Command Shell window. The InstallShield Wizard Complete page appears.

8. Click Finish.

Appendix B Initializing the CA with 1-of-N OCS

To initialize the Entrust Authority Security Manager with a 1-of-N OCS:

1. Open a command prompt and navigate to **C:\Program Files (x86)\Entrust\Security Manager\Bin** and run the command:

```
entsh.exe" -e "source \"C:/Program Files (x86)/Entrust/Security
Manager/etc/FirstTimeInit.tcl\""
```

3. When prompted for the password for the CA hardware, provide the operator card password.

4. When the initialization process is complete, the Entrust Master Control Command Shell informs you that the Entrust infrastructure has been set up.

Contact Us

Web site:	https://www.entrust.com
Support:	https://nshieldsupport.entrust.com
Email Support:	nShield.support@entrust.com
Online documentation:	Available from the Support site listed above.

You can also contact our Support teams by telephone, using the following numbers:

Europe, Middle East, and Africa

United Kingdom:	+44 1223 622444
	One Station Square
	Cambridge
	CB1 2GA
	UK

Americas

Toll Free:	+1 833 425 1990
Fort Lauderdale:	+1 954 953 5229
	Sawgrass Commerce Center – A
	Suite 130,
	13800 NW 14 Street
	Sunrise
	FL 33323 USA

Asia Pacific

Australia:	+61 8 9126 9070
	World Trade Centre Northbank Wharf
	Siddeley St
	Melbourne VIC 3005
	Australia
Japan:	+81 50 3196 4994
Hong Kong:	+852 3008 3188
	31/F, Hysan Place
	500 Hennessy Road
	Causeway Bay
	Hong Kong

To get help with
Entrust nShield HSMs

nShield.support@entrust.com

nshieldsupport.entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

ENTRUST

SECURING A WORLD IN MOTION