ENTRUST

SECURING A WORLD IN MOTION

Entrust Authority Security Manager 8.1 SP1 Patch 197297

nShield® HSM Integration Guide for RHEL 6.x

Version: 1.11

Date: Thursday, November 26, 2020

nCipher Security Limited
Registered Office: One Station Square,
Cambridge, CB1 2GA, United Kingdom
Registered in England No. 11673268

Contents

1 Introduction 5

1.1 Product configurations 5

1.2 Requirements 6

1.3 Credential considerations 7

1.4 This guide 7

1.5 More information 7

2 Procedures 8

2.1 To integrate Entrust Authority Security Manager and HSM: 8

2.2 Installing the nShield Security World Software and creating the Security World 8

2.3 Installing and configuring OpenWave Directory Server 6.0 9

2.3.1 To install Openwave Directory Server 6.0: 9

2.4 Configuring the DSA for use with your Entrust setup 10

2.5 Managing the DSA using odsmgmt 12

2.6 Installing and configuring PostgreSQL Server 9.1.21 13

2.7 Installing and configuring Entrust Authority Security Manager 8.1 SP1 14

2.8 Installing Entrust Authority Security Manager 15

2.9 Configuring Entrust CA 15

2.10 Installing Patch 197297 18

2.11 Initializing the CA with 1-of-N OCS 18

2.12 Initialize the CA with a K-of-N OCS 19

2.13 Moving a CA key pair between software and HSM protection 20

2.14 Exporting the key from hardware to software 20

2.15 Installing Entrust Security Manager Administration 21

2.16 Useful information concerning Operator Card Sets (OCS): 21

2.17 Backup 22

2.18 Restore Entrust to a new server when using an nShield HSM 22

2.18.1 Procedure overview 22

2.18.2 Application software installation on the new server 23

2.18.3 Notes on the SM_81SP1_Operations document: 25

3 Troubleshooting 28
Contact Us 29
Europe, Middle East, and Africa 29
Americas 29
Asia Pacific 29

1 Introduction

Entrust Authority Security Manager is a Public-Key Infrastructure (PKI) that manages digital certificates and can publish Certificate Revocation Lists (CRLs). The nCipher nShield 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 Product configurations

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

Operating System	Entrust version	Security world software version	nShield Connect+	nShield Solo	nShield Edge
RedHat Enterprise Linux 6.6	8.1 SP1 with patch 197297	12.10 (hardserver 3.21.3)	Yes	Yes	Yes

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

Supported nShield functionality	
Function	Supported
Key Generation	Yes
Key Management	Yes
Key Import	-
Key recovery	Yes
1-of-N Operator Card Set	Yes
K-of-N Operator Card Set	Yes
Softcards	Yes
Module-only Key	-

Supported nShield functionality	
Function	**Supported**
Strict FIPS Support	Yes
Load balancing	Yes
Failover	Yes

Fail Over and Load Balancing is not supported with the nShield Edge.

For more information about OS support, contact your Entrust sales representative or nCipher Support. For more information about contacting nCipher, see “Addresses” at the end of this guide. Additional documentation produced to support your nShield product can be found in the document directory of the CD-ROM or DVD-ROM for that product.

1.2 Requirements

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

Role	Operating System
Server - RedHat Enterprise Linux 6.6	nShield Security World Software 12.10 Openwave Directory Server 6.0 PostgreSQL Server 8.3.11 Entrust Authority Security Manager 8.1 with Patch 197297
Client – Windows 7	Entrust Authority Security Manager 7.1 Administration

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.

The nShield Edge does not support NIST SP800-131.

1.3 Credential considerations

- When installing the OpenWave Directory Server (OWDS) three separate passwords will be needed that are a minimum of 8 characters long and consist of both upper and lower case letters and at least 1 numeral
- When installing PostgreSQL Server three separate passwords will be needed that are a minimum of 8 alphanumeric characters as described above
- When initializing the CA five separate passwords will be needed that are a minimum of 10 alphanumeric characters as described above
- When initializing the Directory System Agent (DSA) there are a number of attributes that must be considered beforehand. These include items such as the name of the DSA, the administrator name and associated passwords.

The passwords lengths above are minimum password lengths and nCipher recommends the minimum length should be 12 characters (alphanumeric and special characters).

1.4 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.

1.5 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

2.1 To integrate Entrust Authority Security Manager and HSM:

1. Install the HSM
2. Install the nShield Security World Software and create the Security World, see *Installing the nShield Security World Software and creating the Security World* on page 8
3. Install and configure Openwave Directory Server 6.0, see *Installing and configuring OpenWave Directory Server 6.0* on page 9:
    a. Install Openwave Directory Server 6.0
    b. Configure the Directory System Agent (DSA) for use with your Entrust Authority Security Manager
    c. Manage the DSA using the odsmgmt.
4. Install PostgreSQL Server, see *Procedures* on page 8:
    a. Create the groups and users
    b. Configure the kernel.
5. Install and configure Entrust Authority Security Manager 8.1 Service Pack 1 (SP1), see *Installing and configuring Entrust Authority Security Manager 8.1 SP1* on page 14:
    a. Create Master Users for controlling the Entrust Authority Security Manager
    b. Install Entrust Authority Security Manager
    c. Configure Entrust CA
    d. Installing the Patch 197297 for PostgreSQL Database version 8.3.11 and Entrust Authority Security Manager version 8.1 SP1 Patch 173358(210) (8.1.700.210)
    e. Initialize the CA with 1-of-N OCS
    f. Initialize the CA with K-of-N OCS
    g. Moving a CA key pair between software and HSM protection.
6. Install and configure Entrust Security Manager Administration, see *Installing Entrust Security Manager Administration* on page 21.

2.2 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 /opt/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=opt/nfast/Preload/<filename>
```

The filename is user defined and will be referenced in the pre-load command. For example:

/opt/nfast/bin>Preload -c <OCS Name> -f <pathname to preload file and filename>

When using multiple HSMs 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) PKCS#11 loadsharing should be enabled. This can be done via the cknfastrc file. Using the text editor of your choice, modify the cknfastrc file and set *CKNFAST_LOADSHARING=1* after enabling database hardware protection you should restart the system.

2.3 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
- Manage the DSA using the Directory Server iCon administrator interface.

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.

2.3.1 To install Openwave Directory Server 6.0:

- Install OpenWave Directory Server 6.0
- Configure the DSA for use with your Entrust setup
- Manage the DSA using the Directory Server iCon administrator interface.

Open Wavew 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.

Obtain the Critical Path Directory Server software. Unzip or untar the rpm file and run it:

- Unzip the OpenWave Directory Server 6.0 software
  - gunzip OWMDS-6.0-0-Linux-x86_64.tar.gz
- Extract the installer as mentioned below
  - tar -xvf OWMDS-6.0-0-Linux-x86_64.tar
- Run the rpm file:
  - rpm -ivh OWMDS-6.0-0.x86_64.rpm

Accept all defaults and ensure that the machine's correct name is displayed.

Run the /opt/openwavemessaging/postinstall script to configure your DS installation.

Please consider the following:

- Input the name of an existing user who is to own and administer DS e.g [root]
- Which group will DS administrators belong to? e.g [root]
- Should users in this group be able to run ldap services on low port numbers? [No] (this includes the default port 389, be aware that choosing Yes has potential security implications. If in doubt consult with your security manager)
- The environment variables *ODSRELEASE* and *PATH* need to be set correctly for DS to work. It is advisable to set these in the .bash_profile.root uses /bin/bash, Do you want to update the .bash_profile? e.g Yes.

2.4 Configuring the DSA for use with your Entrust setup

To configure the DSA for use with your Entrust setup, open the command prompt and run the following command:

```
> /opt/openwavemessaging/ds/bin/odsecreate
```

The above commands create a DSA in the current working directory.

You are prompted to provide the information required to get the DSA up and running so that you can get a Directory User Agent (DUA) to bind to it. If you do not know the form in which to enter the information, press Enter without entering any information.

The DUA is a process that accesses the directory service on the behalf of the users and administrators. The DUA communicates with the DSA using the Directory Access Protocol (DAP) or Lightweight Directory Access Protocol.

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	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 number 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
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) ? Initializing the DSA Reading country codes from file iso3166 admin>Reading country codes from file iso3166 admin>Logfile was odscreate.000	n
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=name <enter appropriate CA name> c=<country>
Please enter the name of the CA in the DSA it must be either a country, organization, organizational unit, domain, locality, organizational role, application process or device.	CA = o=<name>, c=<country>
Press return for top entry to be the CA	
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>

Text on Screen	Enter
Initializing the Entrust DSA Changing update log Openwave Messaging Directory Server Demon Reading country codes from file iso3166 admin>admin>Logfile 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 Writing ldap/objectclasses.cfg Writing ldap/syntaxes.cfg Writing ldap/matchingrules.cfg Writing ldap/oidtable.at Writing ldap/oidtable.oc Writing oidslocal odssched 3995 started Please Note >>> ========== The file entrustdirectorysetup.ini has been created, if Entrust software is being run on a Windows platform copy this file to the Windows folder on the machine where the Entrust/Authority Configuration Utility is to be run. Otherwise no further action is required.	

2.5 Managing the DSA using odsmgmt

Management of the DSA is through the odsmgmt command. This command opens the available operations that can be performed in the OpenWave Directory Service (OWDS) instance.

Use the Command:

```
>/opt/openwavemessaging/ds/bin/odsmgmt
```

This will open a list of management operations.

```
-----------------------------
Openwave Messaging Directory Server Management
-----------------------------
 Enter the letter for the management operation required:
 (x) Stop the directory
 (a) Add a process
 (r) Remove a processss
 (v) View the current state of the processes
 (d) Take a diagnostic dump
```

```
(w) Display directories running
(l) Display odssched.log
(m) Monitor odssched.log
(e) Report any errors or warnings that have occurred
(c) Clears any errors or warnings that have occurred
(q) Quit
>v
```

Select the appropriate objective by using the bracket enclosed letter, for example (v)

This will show the current state of associated OpenWave Processes:

```
pid inst action fails state name options
10614 M default 0 ok odsmdsa -d"/"
10615 0 restart this 0 ok odssdsa
10616 1 restart this 0 ok odssdsa
10617 2 restart this 0 ok odssdsa
10618 3 restart this 0 ok odssdsa
10619 0 restart this 0 ok odscommsi
10620 0 restart this 0 ok odsshadi
10621 0 restart this 0 ok odsldap3 -

ldap:389 -ldaps:0 -http:0 -https:0 - charsetv2:iso8859-1
Press Return:
```

2.6 Installing and configuring PostgreSQL Server 9.1.21

To install PostgreSQL Server on the server computer:

1. Download PostgreSQL Server installer from the Entrust TrustedCare online support site for the Linux operating system (SM_81_PostgreSQL_9.1.21_RH_installer.tar).
2. To start installing the PostgreSQL database for Entrust Security Manager 8.1 SP1, untar the setup file SM_81_PostgreSQL_9.1.21_RH _installer.tar in /opt/
3. Change directory (cd) to SM_81_PostgreSQL_9.1.21_RH _installer.
4. Run the script install_postgres.sh.
5. Accept the license agreement for the installation.
6. Accept the default destination folder /opt/entrust for installing the Entrust PostgreSQL Database program files, and then press Enter.
7. Accept all default destination folders for installing other Database files, and then press Enter.
8. Enter the password for the easm_entrust_pg account, and then press Enter
9. Confirm the password for the easm_entrust_pg account, and then press Enter

10. Enter a password for the internal database user account (easm_entrust) and press Enter
11. Confirm the password for the internal database user account (easm_entrust) and press Enter
12. Enter a password for the internal database user account (easm_entbackup) and press Enter
13. Confirm the password for the internal database user account (easm_entbackup) and press Enter
14. Accept the default Database listen port 5432 in the Entrust Authority (TM) Security Manager PostgreSQL, and press Enter.
15. The following message will be displayed if installation is successful: "Installation and configuration of Entrust Authority (TM) Security Manager PostgreSQL Database completed".

2.7 Installing and configuring Entrust Authority Security Manager 8.1 SP1

Create Master Users for controlling the Entrust Authority Security Manager.

Before you install the Entrust Authority Security Manager, create the group entrust and Master users and set the password for it.

Master Users are responsible for controlling the Security Manager software through the Security Manager Control Command Shell. There are three predefined Master User roles:

1. Master1
2. Master2
3. Master3.

These user names are case-sensitive and cannot be changed. The people chosen for these roles must be present when you initialize Security Manager to choose and enter their own unique and private passwords also, they must have physical access to the server that hosts Security Manager, so that they can maintain the Security Manager infrastructure.

These roles appear in the Security Manager software.

Master Users use Security Manager Control Command Shell to:

- Start and stop the Security Manager service
- Backup and restore the Security Manager data files
- Maintain the Certification Authority (CA), including updating the CA keys.

The Primary Group for user account Master1, Master2, Master3 is Entrust.

The Secondary Group for user account Master1, Master2, Master3 is easm_entrust_pg.

To add Masters in Security Manager Server:

- Create group entrust

```
>groupadd -g 505 entrust
```

Create users Master1, Master2 and Master3. Make entrust the primary group and easm_entrust_pg the secondary group of these users:

```
>useradd -g entrust -G easm_entrust_pg Master1
```

```
>useradd -g nfast Master1
```

2.8 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 Linux operating system (SM_81SP1_WithPatch173358_RH_installer.tar).
2. Untar the setup file SM_81SP1_WithPatch173358_RH_installer.tar in /opt/
3. Change directory (cd) to SM_81SP1_WithPatch173358_RH_installer and run script install.sh.
4. Accept the license agreement for the installation.
5. Accept the default destination folder /opt/entrust for installing the Entrust Authority Security Manager program, and then press Enter.
6. Accept the default destination folder /opt/entrust/authdata for installing Security Manager CA data authdata.
7. Enter Master1 as the name of the Linux user that will own the installation.
8. Press Enter. When the installer prompts you to add 'Master1' to the 'easm_entrust_pg' group, press y.
9. Press Enter. When the installer prompts you to configure a CA now, press y.
10. Press Enter twice to proceed with the configuration of Entrust CA.

2.9 Configuring Entrust CA

To configure Entrust CA:

After the installation, press Enter to accept the default full path of the CA data directory.

1. When prompted, enter the Enterprise licensing information that appears on your Entrust licensing card:
    - Serial Number
    - Enterprise user limit

- Enterprise licensing code.

2. When prompted, enter the Web licensing information that appears on your Entrust licensing card:
   - Serial Number
   - Enterprise user limit
   - Enterprise licensing code.
3. Press Enter for Domestic DV Serial Number, Foreign DV Serial Number and IS Serial Number.
4. Enter 1 (LDAP directory) for the type of Directory service.
5. Enter the hostname or IP address of the machine that is hosting the Directory service 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 Configuring the DSA for use with your Entrust setup on page 4) and bind the information:

```
CA DN o=Entrust,c=gb
```

```
CA Directory access password <CA's password>
```

9. Verify the information for the First Officer, and then press Enter:

```
CA DN cn=First Officer, o=Entrust, c=gb
```

11. Enter the information for the Directory Administrator and bind the information:

```
CA DN cn=diradmin
```

```
Directory access password <Administrator's password>
```

14. Press Enter to accept default values when prompted for the following:
    - Entrust Proto-PKIX (PKIX) port [709] :
    - Entrust Administration Protocol (ASH) port [710] :
    - Certificate Management Protocol (PKIX-CMP) port [829] :
    - Entrust XML Administration Protocol (XAP) port [443] :
    - Enable XAP service? (y/n) ? [y]
15. When the installer prompts "Are you using a hardware device for the CA keys (y/n) ? [n]",type y.
16. When prompted, enter the pathname for the CryptokiLibrary as /opt/nfast/toolkits/pkcs11/libcknfast.so.

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

    Example: nCipher Corp. Ltd SN : 331688d2fb5166be SLOT : 761406613

18. In the Cryptographic Information section, select settings as appropriate, for example:

Cryptographic Information	Settings
CA Key Type for signing operations	RSA
RSA type and corresponding key length	RSA-2048
Algorithm for signing operations	RSA-SHA256
Type of key pair that will be used for user signing and nonrepudiation keys	RSA type and corresponding key length
RSA type and corresponding key length	RSA-2048
Type of key pair that will be used for user encryption and dual usage key pairs	RSA
RSA type and corresponding key length	RSA-2048

19. When the installer prompts 'Do you wish to work with Microsoft (R) Windows (R) applications? (y/n) ? [n]', accept the default by pressing **Enter**
20. Enter the password that was assigned to easm_entrust when you installed the PostgreSQL Server 8.3.11 (see Installing PostgreSQL Server 8.3.11), and then press **Enter**
21. Enter the password that was assigned to the backup user when you installed the PostgreSQL Server 8.3.11 (see Installing PostgreSQL Server 8.3.11), and then press **Enter**.
22. Accept the defaults for the algorithm that will be used for database encryption.
23. When prompted, select RootCA to create a Root Certificate Authority.
24. When the installer prompts for the following, accept the defaults by pressing **Enter**:

    CA certificate lifetime 120
    CA private key usage period 100
    policy certificate lifetime in days 30

25. Verify the information and type 'yes' to finish configuration.

    

    For any error during the configuration process, type the section number to review the details.

26. Select 2 to exit the installation and configuration and initialize the CA later.

2.10 Installing Patch 197297

Installing the Patch 197297 for PostgreSQL Database version 8.3.11 and Entrust Authority Security Manager Version 8.1 SP1 Patch 173358(210) (8.1.700.210).

Before applying the patch 197297 make sure Entrust Authority (TM) PostgreSQL Database version 8.3.11 and Security Manager version 8.1 SP1 Patch 173358(210) (8.1.700.210) is installed.

1. Upgrade the Entrust Authority (TM) PostgreSQL Database version 8.3.11 to the new version 9.1.21
    a. Login as root user
    b. Download SM_81SP1_PostgreSQL_9121_RH_installer.tar for RHEL
    c. Run the tar command **tar -xf <downloaded tar file>** to extract the contents of the install package. The tar command will create: **SM_81SP1_PostgreSQL<version>_<platform>_installer** folder where the installer will be located
    d. cd SM_81SP1_PostgreSQL<version>_<platform>_installer and invoke the installer with the command **./install_postgres.sh**, follow the steps of the installer.
2. Upgrade the Entrust Authority (TM) Security Manager version 8.1 SP1 Patch 173358 (210) (8.1.700.210) to the new version Security Manager 8.1 SP1 patch 197297.
    a. Login as root user
    b. Download SM_81SP1_197297_RH.tar.gz for RHEL
    c. Extract the contents of the installer package by gunzip and untar.

    The tar command will create SM_81SP1_197297_RH folder.

    d. Run the **./install.sh**, follow the steps of the installer.

2.11 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 login as Master1
2. Source the file **/opt/entrust/authdata/CA/env_settings.sh** (or env_settings.csh)
3. Run the command:

```
entsh -e "source /opt/entrust/authority8.1sp1/etc/FirstTimeInit.tcl"
```

5. When prompted for the passwords for Master1, Master2, Master3 and First Officer, provide the specified passwords.

When setting passwords for Master users and the First Officer note the following constraints: the password must be at least 10 characters in length and not based on a dictionary word. Further, the characters must be both a mix of upper and lower case and include numbers

6. When prompted for the password of the CA hardware, give the passphrase of the 1-of-N Operator Card Set.
7. When the initialization process is complete, the Entrust Master Control Command Shell informs you that the Entrust infrastructure has been set up. Press Return to exit.

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

2.12 Initialize the CA with a K-of-N OCS

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

1. Create an empty file within folder /opt/nfast/, for example: /opt/nfast/kofn.
2. Edit the file cknfastrc located in /opt/nfast and add the following environment variable:

```
NFAST_NFKM_TOKENSFILE=location of the empty file (kofn) in /opt/nfast/ folder
```

4. Open the command prompt in one session and preload the cardset by running the following command:

```
/opt/nfast/bin/preload -c cardsetname -f <file location mentioned in nfast variable
NFAST_NFKM_TOKENSFILE> pause
```

6. Type the passwords for the OCS.
7. Open another command prompt and source the file /opt/entrust/authdata/CA/env_settings.sh (or env_settings.csh).
8. Run the command:

```
entsh -e "source /opt/entrust/authority8.1sp1/etc/FirstTimeInit.tcl"
```

10. When prompted for the passwords for Master1, Master2, Master3 and First Officer, provide the specified passwords.
11. When prompted for the password of the CA hardware, give the passphrase of the K-of-N Operator Card Set.
12. When the initialization process is complete, the Entrust Master Control Command Shell informs you that the Entrust infrastructure has been set up. Press Return to exit.

2.13 Moving a CA key pair between software and HSM protection

The following procedures are described in this section:

- Importing the CA key pair to the HSM (from software to hardware)
- Exporting the CA key pair from the HSM (from hardware to software).

Before performing either procedure, log in as Master 1 to check that the Entrust Master Control shell is running.

Importing the key from software to hardware

To import the CA key pair from software to the HSM:

1. Open the Entrust Authority Master Control shell.
2. Begin updating the keys by running the command:

```
entsh$ ca key update
```

This prompts you to select the destination for the new CA key.

4. Select the nCipher slot as the destination for the new CA key. For example:
   a. software
   b. nCipher Corp. Ltd SN: ec7759a6ecc0b7f0 SLOT: 7614066133
   c. Cancel operation

      >2

   d. To continue to update the CA key, type `y` .

After you have moved the CA key to the HSM and have finished updating it, a message about the CA profile being successfully recovered appears. The Entrust Authority Security Manager configuration and integration with the HSM is now complete.

2.14 Exporting the key from hardware to software

To export the Entrust CA key pair from the HSM to software:

1. Open the Entrust Authority Master Control shell.
2. Begin updating the keys by running the command:

```
entsh$ ca key update
```

This prompts you to select the destination for the new CA key.

4. Select the software slot as the destination for the new CA key. For example:
    a. software
    b. nCipher Corp. Ltd SN: ec7759a6ecc0b7f0 SLOT: 7614066133
    c. Cancel operation

       >1

    d. To continue to update the CA key, type y .

After you have finished updating the CA key, its export to software is complete.

2.15 Installing Entrust Security Manager Administration

Entrust Security Manager Administration is a Microsoft only application and provides a graphical user interface for administrators of Entrust Security Manager. It is used for creating Entrust profiles, defining their roles, and applying security policies. The following activities should be performed on a Windows 2012 R2 or Windows 7 server instance.

To install the Entrust Security Manager Administration to work with Entrust Authority Security Manager:

1. Before install copy the authdata /opt/entrust/authdata/ folder from your Linux server to a suitable Microsoft Windows server, running at least Windows 2012 R2
2. Synchronize the date and time
3. Ensure that the IP address is set correctly and that all permissions are at the appropriate values
4. Run the setup file: SMA_81SP1_setup.exe
5. Click Next
6. While installation give the path of windows folder
7. To complete the installation, click Finish
8. Restart the client (Windows Server 2012 R2 or Windows 7) to ensure that the new .ini files and profiles are detected
9. Select Start > Programs > Entrust Security Administrator
10. Click Find Profile and, in the Browse window, navigate to C:\Windows\epf
11. Select First Officer.epf and click Open, which closes the Browse window
12. Type the password for First Officer.epf and click OK to log in to the application.

2.16 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
  - clear the module.

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

2.17 Backup

You must ensure that the Security world /local directory in opt/nfast/kmdata/local is backed up after any Security World administration activities and key generation, deletion etc. and that the backups are stored securely under your change control process.

2.18 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 Security World kmdata/local directory and the Entrust Security Manager Backup (mgrbkYYYYMMDDHHMMSS).

2.18.1 Procedure overview

1. Build the new 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 opt/nfast/
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.

2.18.2 Application software installation on the new server

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

Install the new Operating System onto the server. When building the new server, ensure that it is as close to replicating the old (deprecated) server (i.e. 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.

1. 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
2. Install OpenWave Directory services on the new server
3. Initialize the DSA with the same settings as on the original server
4. Install PostgreSQL on the new server.

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

```
opt/nfast/bin>enquiry 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
```

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

```
opt/nfast/kmdata/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:

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

```
opt/nfast/bin>nfkminfo
```

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

```
opt/nfast/bin>nfkminfo
 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
```

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

```
opt/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 utilizing multiple Security Worlds in your environment (if in doubt contact nCipher support

Open the cknfastrc file with a text editor and edit to include the entries shown below:

```
opt/nfast/cknfastrc
```

```
CKNFAST_NO_UNWRAP=1
CKNFAST_NO_ACCELERATOR_SLOTS=1
CKNFAST_LOADSHARING=1
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none
NFAST_NFKM_TOKENSFILE=opt/nfast/Preload/<preload_filename>
```

NFAST_NFKM_TOKENSFILE=opt/nfast/Preload/<preload_filename>. The <filename> must be the same as on the original server. Once the edits (see above) have been made save the file and close the editor.

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

```
opt/nfast/bin>nfkminfo -k
```

Run the nShield preload session.

```
opt/nfast/bin>preload.exe -c OCS_name -f <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.

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.

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.

2.18.3 Notes on the SM_81SP1_Operations document:

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.

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 rolesas per the example below:

```
C[login]
maxProcs=256
. .
. .

dbloginpw=Password
dbBackupPw=Password
```

Remember to save the file and exit.

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, belwo is an example of the authauto.ini file after dbloginpw and dbBackupPw credentials removed.

```
[dbloginpw Credentials]

[Hardware Info]
CAKey=6E43697068657220436F72702E204C74642020534E203A20393731633030306534
_continue_=61363934353739
DbProt=2020534E203A20
HwList=6E43697068657220436F72702E204C74642020534E203A203937316330303065 3
_continue_=461363934353739X

[dbBackupPw CredentialsC[login]
```

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	Solution
Error encountered querying CA hardware.	Red Hat Enterprise Linux 6.4 and Security World Software version is 64 bit but Entrust version is 32 bit	Install 32bit components over 64 bit Security World Software and make sure 32bit PKCS #11 library(libcknfast.so) located at /opt/nfast/toolkits/pkcs11/ or Manually copy the 32bit PKCS #11 library libcknfast.so library from 32 bit Security World Software
(-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$).	Start the entrust service from entsh by running the command >service start
(-2684) General hardware error	ncipher service is stopped or not running.	Start the nfast service by running the command from /opt/nfast/sbin/init.d-ncipher restart
First officer is not able logged into SMA	Permission issue on EPF file.	Check the permission of files in epf folder and make sure on server and client has the same the date/time
(-2229) An error occurred. Check the service status and manager logs for details	Timeout	Login to entsh and run service status, if the service is shown as down start the service with service start

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