Entrust Authority Security Manager 10

nShield® HSM Integration Guide for Linux

17 Dec 2021

Contents

1. Introduction

The Entrust Authority Security Manager is a Public-Key Infrastructure (PKI) solution. The Entrust nShield Hardware Security Module (HSM) securely store and manage encryption keys. This document describes how to integrate both for added security of your PKI.

The HSM is available as an appliance or software as a service (SaaS). Throughout this guide, the term HSM refers to nShield Solo, nShield Connect, and nShield Edge products.

1.1. Product configuration

Entrust tested the integration with the following versions:

Product	Version
Entrust Security Manager	v10.0.10
PostgreSQL	v11_7_RH8
Red Hat Enterprise Server	v8.3

1.2. Supported nShield hardware and software versions

Entrust tested the integration with the following nShield HSM hardware and software versions:

Product	Security World	Firmware	Netimage
Connect XC	12.80.4	12.50.11	12.80.4
Connect Plus	12.80.4	12.50.8	12.80.4
Edge	12.80.4	12.50.11	NA

1.3. Requirements

Familiarize yourself with:

- The Entrust Security Manager (https://www.entrust.com/digital-security/certificate-solutions/products/pki/security-manager).
- The nShield HSM: *Installation Guide* and *User Guide*.
- Your organizational Certificate Policy and Certificate Practice Statement, and a Security Policy or Procedure in place covering administration of the PKI and HSM:

- 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 Operator Card Set (OCS), and the policy for managing these cards.
- The keys protection method: Module, Softcard, or OCS.
- The level of compliance for the Security World, FIPS 140-2 Level 3.
- Key attributes such as key size, time-out, or need for auditing key usage.

2. Procedures

Prerequisites:

- A dedicated Linux server for the installation.
- Access to TrustedCare Portal (to download Software) https://trustedcare.Entrust.com/.

Steps:

1. Install the HSM
2. Install the nShield Security World Software and create the Security World
3. Generate the OSC or Softcard in the CA server
4. Install and configure Directory Services
5. Install the Entrust Authority database
6. Create Master Users for controlling the Security Manager software
7. Install the Security Manager
8. Establish a preload session
9. Prepare the Entrust Security Manager configuration info
10. Configure the Entrust Security Manager
11. Initialize Security Manager
12. Launch a Security Manager Shell
13. Show the Security Manager status
14. Import key from the Entrust Security Manager database to the HSM
15. Export the key from the HSM to the Entrust Security Manager database
16. List all the keys
17. List all the certificates
18. Back up Security World files

2.1. Install the HSM

Install the nShield Connect HSM locally, remotely, or remotely via the serial console. See the following nShield Support articles, and the *Installation Guide* for the HSM:

- https://nshieldsupport.entrust.com/hc/en-us/articles/360021378272-How-To-Locally-Set-up-a-new-or-replacement-nShield-Connect
- https://nshieldsupport.entrust.com/hc/en-us/articles/360014011798-How-To-Remotely-Setup-a-new-or-replacement-nShield-Connect
- https://nshieldsupport.entrust.com/hc/en-us/articles/360013253417-How-To-

2.2. Install the nShield Security World Software and create the Security World

1. Install the Security World software as described in *Installation Guide* and the *User Guide* for the HSM. This is supplied on the installation disc.
2. Add the Security World utilities path `/opt/nfast/bin` to the system path.
3. Open the firewall port 9004 for the HSM connections.
4. 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_OVERRIDE_SECURITY_ASSURANCES=none
```

When using a K-of-N Card Set where K>1, set `CKNFAST_LOADSHARING=0`. When using a K-of-N Card Set where K=1, set `CKNFAST_LOADSHARING=1`. This also applies to when using Softcards.

When you are using nShield with ePassport CVCA, use `CKNFAST_ASSUME_SINGLE_PROCESS=0`. If ePassport Document Verifier Certificate requests are canceled, this setting ensures that the associated physical key is deleted in the HSM. For information on environment variables, see the *User Guide* for the HSM.

5. Open a command window and run the following to confirm the HSM is `operational`.

```
# enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        530E-02E0-D947 7724-8509-81E3 09AF-0BE9-53AA 9E10-03E0-D947
 mode                 operational
...
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        530E-02E0-D947
 mode                 operational
 ...
```

6. Create your Security World if one does not already exist, or copy an existing one. Follow your organization's security policy for this. Create extra ACS cards as spares in case of a card failure or a lost card.

ACS cards cannot be duplicated after the Security World is created.

7. Confirm the Security World is `usable`.

```
# nfkminfo
World
 generation  2
 state       0x37270008 Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
```

2.3. Generate the OSC or Softcard in the CA server

The OCS or Softcard and associated passphrase will be used to authorize access to the keys protected by the HSM. Typically, one or the other will be used, but rarely both. Follow your organization's security policy to select which one to use.

2.3.1. Create the OCS

1. Ensure file `/opt/nfast/kmdata/config/cardlist` contains the serial number of the card(s) to be presented, or the wildcard "*".
2. Open a command window as administrator.
3. Run the `createocs` command as described below, entering a passphrase or password at the prompt.

   Follow your organization's security policy for this for the values K/N, where K=1 as mentioned above. Use the same passphrase for all the OCS cards in the set (one for each person with access privilege, plus the spares). Note that `slot 2`, remote via a Trusted Verification Device (TVD), is used to present the card.

After an OCS card set has been created, the cards cannot be duplicated.

```
# createocs -m1 -s2 -N EntrustSM -Q 1/1

FIPS 140-2 level 3 auth obtained.

Creating Cardset:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: Admin Card #1
 Module 1 slot 2: empty
 Module 1 slot 3: empty
 Module 1 slot 2: blank card
 Module 1 slot 2:- passphrase specified - writing card
Card writing complete.

cardset created; hkltu = 201f114b435dbe89eeeae484412e2266b4da2abe
```

Add the **-p** (persistent) option to the command above to have authentication after the OCS card has been removed from the HSM front panel slot, or from the TVD. The authentication provided by the OCS as shown in the command line above is non-persistent and only available while the OCS card is inserted in the HSM front panel slot, or the TVD.

4. Verify the OCS was created.

```
# nfkminfo -c
Cardset list - 1 cardsets:  (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
 Operator logical token hash               k/n timeout  name
 201f114b435dbe89eeeae484412e2266b4da2abe  1/1  none-NL EntrustSM
```

The `rocs` utility also shows the OCS was created.

```
# rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cardset
No. Name                    Keys (recov) Sharing
  1 EntrustSM               0 (0)        1 of 1
rocs> quit
```

2.3.2. Create the Softcard

1. Add the line below to the `/opt/nfast/cknfastrc` file for Softcard support. Create the file if it does not exists.

```
CKNFAST_LOADSHARING=1
```

2. Run the following command, and enter a passphrase or password at the prompt.

```
# ppmk -n EntrustSNSoftcard

Enter new pass phrase:
Enter new pass phrase again:
New softcard created: HKLTU cc92a2d25a9c78d4cd8c2d4bbb95c4401f9f6be1
```

3. Verify the Softcard was created.

```
# nfkminfo -s
SoftCard summary - 1 softcards:
 Operator logical token hash               name
 cc92a2d25a9c78d4cd8c2d4bbb95c4401f9f6be1  EntrustSNSoftcard
```

The `rocs` utility also shows that the OCS and Softcard were created.

```
# rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cardset
No. Name                    Keys (recov) Sharing
  1 EntrustSM           0 (0)        1 of 1
  2 EntrustSMSoftcard   0 (0)        (softcard)
rocs> quit
```

2.4. Install and configure Directory Services

1. Make a note of the following parameters of your existing Directory Services:
   - Top Level DN: `o=Entrust`
   - CA Directory Location: `ou=CA,o=Entrust`
   - Director Administrator: `cn=diradmin,ou=CA,o=Entrust`
   - Password for CA: xxxxxx
   - Password for Directory Administrator: xxxxxx

   Alternatively, install Directory Services locally or in another server. Follow the instructions in the *Entrust Authority Security Manager 10.0 Directory Configuration Guide* for a new installation.

2. If you are accessing a Directory Service in another server, add the following rule to the firewall:

```
firewall-cmd --add-port=389/tcp
```

3. Test access to the Directory Services:

```
ldapsearch -x -h <directory_services_server_IP> -p 389 -b "cn=diradmin,ou=CA,o=Entrust"
```

```
# ldapsearch -x -h 10.194.148.96 -p 389 -b "cn=diradmin,ou=CA,o=Entrust"
# extended LDIF
#
# LDAPv3
# base <cn=diradmin,ou=CA,o=Entrust> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# diradmin, CA, Entrust
dn: cn=diradmin,ou=CA,o=Entrust
cn: diradmin
sn: Administrator
objectClass: top
objectClass: person
objectClass: organizationalPerson
    objectClass: inetOrgPerson
userPassword:: ZW50UEtJMjAwMA==

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

2.5. Install the Entrust Authority database

Entrust Security Manager requires a database to store information about the Certification Authority, X.509 users, and EAC entities. For a list of supported databases, see the product document *PSIC-Entrust Authority Security Manager 10.0* on Entrust TrustedCare.

An embedded Security Manager PostgreSQL database is used for the purpose of this guide. This database will be installed on the same server that will host Security Manager.

Entrust strongly recommends that you install your own supplied database on its own dedicated server. To install and configure (or upgrade) your chosen database, read your database documentation and the *Security Manager Database Configuration Guide*.

Use your own database to install and use Security Manager in a cluster. The Entrust supplied Security Manager PostgreSQL Database is not supported for a cluster environment.

1. Download the PostgreSQL Server installation files (`SM_PostgreSQL_11_7_RH8_installer.tar.gz`) from the Entrust TrustedCare online support site.
2. Extract the TAR file to a directory.

```
% mkdir postgres
% cd postgres
% tar zxvf SM_PostgreSQL_11_7_RH8_installer.tar.gz
```

3. Navigate to the directory where you extracted the TAR file and start the installation:

```
% cd SM_PostgreSQL_11_7_RH8_installer
% sudo ./install_postgres.sh
```

   Accept all defaults during the installation. The installer generates the following log file: `/tmp/pg_install.log`.

   This process creates three users:

   - PostgreSQL user account: `easm_entrust_pg`
   - PostgreSQL database account: `easm_entrust`
   - PostgreSQL backup database account: `easm_entbackup`

Make a note of these users and passwords.

2.6. Create Master Users for controlling the Security Manager software

Master Users are responsible for controlling the Security Manager software through the Security Manager Control Command Shell.

There are three predefined Master User roles: `Master1`, `Master2`, and `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, so they can 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.

Master Users use Security Manager Control Command Shell to:

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

The Primary Group for user accounts `Master1`, `Master2`, `Master3` is `easm_entrust_pg`. The Secondary Group for user accounts `Master1`, `Master2`, `Master3` is `entrust`. These users must also belong to the `nfast` group.

By default, the Security Manager PostgreSQL Database installer creates the `easm_entrust_pg` group.

1. Create the groups needed for Security Manager.

   All user accounts that you create for Security Manager must belong to the same

group. Create these group before you create any user accounts for Security Manager.

```
% sudo groupadd entrust
% sudo groupadd easm_entrust_pg
```

2. Create the Master users:

```
% sudo useradd -c "Master User 1" -g easm_entrust_pg Master1
% sudo useradd -c "Master User 2" -g easm_entrust_pg Master2
% sudo useradd -c "Master User 3" -g easm_entrust_pg Master3
```

3. Add users to groups:

```
% sudo usermod -a -G entrust Master1
% sudo usermod -a -G nfast Master1
% sudo usermod -a -G entrust Master2
% sudo usermod -a -G nfast Master2
% sudo usermod -a -G entrust Master3
% sudo usermod -a -G nfast Master3
```

4. Set the users passwords:

```
% sudo passwd Master1
% sudo passwd Master2
% sudo passwd Master3
```

2.7. Install the Security Manager

1. Download Security Manager Linux (`security-manager-10.0.1-4.el8.x86_64.rpm`) from the Entrust TrustedCare online support site.
2. Run the installer. Use the **-i** option for a new installation, or the **-U** option to upgrade the package currently installed to a newer version.

```
# rpm -U Downloads/security-manager-10.0.10-201.el8.x86_64.rpm
warning: Downloads/security-manager-10.0.10-201.el8.x86_64.rpm: Header V4 RSA/SHA256 Signature, key ID ac33653e:
NOKEY
   Verifying OS support...
   OS is a supported OS.


%easm_entrust_pg ALL=(Master1) NOPASSWD: /opt/entrust/authority/bin/entsm_initd.sh
   Checking Security Manager service status
```

2.8. Establish a preload session

The OCS or the Softcard must be preloaded to configure the Security Manager.

1. Create an empty file within folder `/opt/nfast/`, for example: `/opt/nfast/entrustsmtoken`. This is the token file.

   

   Restrict access permissions to the token file to authorized persons. Otherwise it presents a security risk.

2. Edit the file `/opt/nfast/cknfastrc` and add the following environment variable set to the location of the file created above:

   ```
   NFAST_NFKM_TOKENSFILE=/opt/nfast/entrustsmtoken
   ```

3. Open a command window to run preload exclusively.

   

   Do not close this window throughout the Entrust Security Manager configuration. Otherwise the configuration will fail.

4. Preload the Card Set by running the `preload -c` command for OCS, or `preload =s` command for Softcard.

   ```
   # preload -<c/s> <OCS/Softcard> -f <location of file above> pause
   ```

   Present the OCS cards and passphrase when prompted.

   For example:

   ```
   # preload -c EntrustSM -f /opt/nfast/entrustsmtoken pause
   2021-12-13 17:45:39: [89298]: INFO: Preload running with: -c EntrustSM -f /opt/nfast/entrustsmtoken pause
   2021-12-13 17:45:40: [89298]: INFO: Created a (new) connection to Hardserver
   2021-12-13 17:45:40: [89298]: INFO: Modules newly usable: [1].
   2021-12-13 17:45:40: [89298]: INFO: Found a change in the system: an update pass is needed.
   2021-12-13 17:45:40: [89298]: INFO: Loading cardset: EntrustSM in modules: [1]

   Loading `EntrustSM':
    Module 1 slot 2: `EntrustSM' #1
    Module 1 slot 0: Admin Card #1
    Module 1 slot 3: empty
    Module 1 slot 2:- passphrase supplied - reading card
   Card reading complete.

   2021-12-13 17:45:45: [89298]: INFO: Stored Admin key: kfips (21bc...) in module #1
   2021-12-13 17:45:45: [89298]: INFO: Loading cardset: Cardset: EntrustSM (201f...) in module: 1
   2021-12-13 17:45:45: [89298]: INFO: Stored Cardset: EntrustSM (201f...) in module #1
   2021-12-13 17:45:45: [89298]: INFO: Maintaining the cardset EntrustSM protected
   key(s)=['pkcs11:uc201f114b435dbe89eeeae484412e2266b4da2abe-d5ba2a26cc7c33b287bfe005e5a0b3df72be4a5c',
   'pkcs11:uc201f114b435dbe89eeeae484412e2266b4da2abe-5364ff3b878b1b168819a5b40a7b5d13e2465eb9',
   'pkcs11:uc201f114b435dbe89eeeae484412e2266b4da2abe-c516ece5ccedac4bc3e4ca5862e12a9eb58cc945'].
   2021-12-13 17:45:45: [89298]: INFO: The private/symmetric key pkcs11/uc201f114b435dbe89eeeae484412e2266b4da2abe-
   d5ba2a26cc7c33b287bfe005e5a0b3df72be4a5c is loaded in module(s): [1].
   2021-12-13 17:45:45: [89298]: INFO: The private/symmetric key pkcs11/uc201f114b435dbe89eeeae484412e2266b4da2abe-
   5364ff3b878b1b168819a5b40a7b5d13e2465eb9 is loaded in module(s): [1].
   2021-12-13 17:45:45: [89298]: INFO: The private/symmetric key pkcs11/uc201f114b435dbe89eeeae484412e2266b4da2abe-
   c516ece5ccedac4bc3e4ca5862e12a9eb58cc945 is loaded in module(s): [1].
   2021-12-13 17:45:45: [89298]: INFO: Loading complete. Now pausing...
   ```

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.

5. Confirm the OCS or Softcard has been preloaded by opening a separate command window and running the following command.

```
# preload -<c/s> <OCS/Softcard> -f <location of file above> nfkminfo
```

For example:

```
# preload -c EntrustSM -f /opt/nfast/entrustsmtoken nfkminfo

...

Pre-Loaded Objects (  5):  objecthash   module objectid  generation
 619111a00b99f3cc51921822c83e42420136028d   1 0xabb5109c 1
 02186fd5fb53ddc88172a62e16b4e006a459d02c   1 0xabb5109b 1
 06dc5a4dfdada00ff9fd20937eee002e84264f0c   1 0xabb5109a 1
 201f114b435dbe89eeeae484412e2266b4da2abe   1 0xabb51099 1
 21bc55568efdcb586e969804122149d3222ef19e   1 0xabb510a0 1
```

2.9. Prepare the Entrust Security Manager configuration info

The Entrust Security Manager configuration is an interactive process to choose certificate algorithms, lifetimes, and other options for your Certification Authority. Choose and/or enter the information as show below.

Database Deployment model

- Select **1** for the database deployment model.

Authdata Directory

- Select **Enter** to accept default values when prompted for the installation directory for the Security Manager CA data (`authdata`).

CA Data Directory

- Select **Enter** to accept default values when prompted for the CA data directory.

Licensing Information

- Enter the Enterprise licensing as it appears on your Entrust licensing card:
  - Serial Number.

    - Enterprise user limit.
    - Enterprise licensing code.
- Enter the Web licensing as it appears on your Entrust licensing card:
    - Serial Number.
    - Enterprise user limit.
    - Enterprise licensing code.
- Select **Enter** for Domestic DV Serial Number, Foreign DV Serial Number, and IS Serial Number.

Directory Communications

- Enter **1 (LDAP directory)** for the type of Directory service.
- Enter the hostname or IP address of the server hosting the Directory Services and directory listen port (**389**).

CA Distinguished Names (DNs)

- Enter the distinguished name (DN) and password of the Certificate Authority (CA) entry in your Directory provided when configuring the Directory Services.

DN of CA	**ou=CA,o=Entrust**
CA password	*<CA's password>*

- Verify the information for the First Officer, select **Enter**:

CA DN	**cn=First Officer,ou=CA,o=Entrust**

Directory Administrator

- Enter the Distinguished Name and password of the Directory Administrator (DA) provided when configuring the Directory Services.

DN of DA	**cn=diradmin,ou=CA,o=Entrust**
DA password	*<Administrator's password>*

TCP Communication Ports

- Select **Enter** to accept all the defaults:
    - **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]:**

CSCA Configuration

- Enter **n** when prompted, **Is this a Country Signing CA (CSCA) (y/n) ? [n]**.

Algorithms

- Enter **y** when prompted **Are you using a hardware device for the CA keys (y/n) ? [n]**.
- For the CryptokiLibrary path, enter `/opt/nfast/toolkits/pkcs11/libcknfast.so`.
- Select the appropriate slot for the desired type of protection.

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

- Select per the table below for the remaining of the **Algorithms** section.

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 for signing and non-repudiation keys.	RSA
RSA type and corresponding key length	RSA-2048
Type of key pair for encryption and dual usage key pairs.	RSA
RSA type and corresponding key length	RSA-2048

Compatibility with Microsoft applications

- Enter **n** when prompted **Do you wish to work with Microsoft ® Windows ® applications? (y/n) ? [n]**.

CRL Distribution Points (CDP) and Combined CRL * Enter **y** when prompted **Do you want to enable automatic login (y/n) ? [n]**.

Database Parameters

- Enter the password that was assigned to `easm_entrust` when you installed the PostgreSQL Server, and then select **Enter**.
- Enter the password that was assigned to the backup user when you installed the PostgreSQL Server, and then select **Enter**.

- Accept the defaults for the algorithm that will be used for database encryption.

CA Parameters

- Select **RootCA** to create a Root Certificate Authority.
- Accept the defaults for CA certificate lifetime and CA private key usage period.

Policy Certificate Lifetime

- Accept the default for policy certificate lifetime.

Automatic Login

- Enter **y** when prompted **Do you want to enable automatic login (y/n) ? [n]**

Security Manager 10.0.1 Configuration Review

- Review the selections made. Enter a section to change or correct typos, or enter **yes** to finish.
- Enter **y** when prompted **Would you like to verify the Directory information (y/n) ? [y]**.
- Select **Enter** to use the default of the full path of the customized certificate specifications file.
- Select **1** to perform the first time initialization and start the CA.
- Enter the OCS or Softcard passphrase when prompter.
- Enter the passwords for `Master1`, `Master2`, and `Master3`.

2.10. Configure the Entrust Security Manager

1. Preload the OCS or Softcard as described in Establish a preload session if you have not done this yet.
2. Test access to the Directory Service from the Security Manager server:

```
# ldapsearch -x -h <directory_services_server_IP> -p 389 -b "cn=diradmin,ou=CA,o=Entrust"
```

3. Become the `Master1` user:

```
% sudo su - Master1
```

4. Navigate to the Security Manager's `\bin` directory:

```
% cd /opt/entrust/authority/bin
```

5. Invoke the configuration shell script. Enter the information required per the section above.

```
% ./config_authority.sh
```

Enter the information required when prompted. If you enter a typo, continue. These can be corrected towards the end, or by editing the `/opt/entrust/authdata/CA/manager/entmgr.ini` before committing.

The following example shows the interactive session of running the shell script.

```
This program will ask you for the information necessary to initialize an
Entrust Certification Authority. At the end of the questionnaire, you will
have the opportunity to review the information, make changes, and verify that
the Directory configuration is correct before commencing with the
initialization of the Certification Authority.
Press <Enter> when you are ready to continue.

We have set your environment locale to en_US.iso885915. Please ensure that your
terminal is appropriately configured, and press <Enter> to continue. Note that
your environment locale will revert to its original setting once this script is
complete.

SM_Configure: Found PG Installation - /home/easm_entrust_pg/.pg_installrc.
SM_Configure: Found PG Settings - PGDATA=/var/pgsql/easm_entrust_pg_data_11,
PGWAL=/var/pgsql/easm_entrust_pg_wal_11,
PGDIR=/opt/entrust/easm_postgresql_11.7.
Detected an existing installation of Entrust Authority (TM) Security Manager
PostgreSQL Database on this host.

Enter the desired database deployment model.
Select one of the following:
         1. embedded
         2. customer-supplied
> 1

================================================================================
Authdata Directory
================================================================================

By default, the Security Manager CA authdata directory will be
'/opt/entrust/authdata'. You may select a different authdata directory. If the
selected directory is not '/opt/entrust/authdata', a symbolic link
'/opt/entrust/authdata' that points to the selected authdata directory will be
created.
Enter the installation directory for Security Manager CA data (authdata).
[/opt/entrust/authdata]


================================================================================
CA Data Directory
================================================================================

Checking for existing CA data directory...

Creating CA data directory...

The CA data directory is for storing CA related data. By default, the CA data
directory will be created as '/opt/entrust/authdata/CA'.

Enter the full path of the CA data directory.
[/opt/entrust/authdata/CA] >
Created the CA data directory /opt/entrust/authdata/CA.
```

```
Preparing subdirectories in '/opt/entrust/authdata/CA'...
Updating /home/easm_entrust_pg/sm_pg.sh...


================================================================================
Licensing Information
================================================================================

Enter the Enterprise licensing information that appears on your Entrust
licensing card.
Serial Number:              xxxxxxx
Enterprise User Limit:      xxxxx
Enterprise Licensing Code:  XXXXXXX

Enter the Web licensing information that appears on your Entrust licensing
card. This is optional at this time. The information may be added at a later
date through Security Manager Administration.
Web Serial Number:          xxxxxxx
Web User Limit:             xxxxx
Web Licensing Code:         XXXXXXX

Enter the CVCA licensing information for domestic DVs that appears on your
Entrust licensing card. This is optional at this time. The information may be
added at a later date by modifying the entmgr.ini file.
Domestic DV Serial Number:

Enter the CVCA licensing information for foreign DVs that appears on your
Entrust licensing card. This is optional at this time. The information may be
added at a later date by modifying the entmgr.ini file.
Foreign DV Serial Number:

Enter the DV licensing information for Inspection Systems that appears on your
Entrust licensing card. This is optional at this time. The information may be
added at a later date by modifying the entmgr.ini file.
IS Serial Number:

================================================================================
 Directory Communications
================================================================================

Enter the type of Directory service.
Select one of the following:
         1. LDAP Directory
         2. Microsoft (R) Active Directory (R)
         3. Microsoft Active Directory Lightweight Directory Services
[1] >1

Enter the hostname or IP address of the machine that is hosting your Directory
service.
[entrustsm-redhat-8] > xx.xxx.xxx.xx

Enter the Directory TCP port number.
[389] >

================================================================================
 CA Distinguished Names (DNs)
================================================================================

IMPORTANT: The countryName (c) attribute for all distinguished names (DNs) will
be converted to uppercase by Security Manager according to ISO/IEC 3166
regardless of the case entered now or the case in the Directory.

Enter the distinguished name (DN) of your Certification Authority (CA) entry in
your Directory. If there isn't already a CA DN entry in the Directory, exit
this program and create one. Enter the CA DN exactly as it appears in the
Directory.
[o=Your Company,c=US] > ou=CA,o=Entrust

Enter the password for this Certification Authority (CA). Use the same password
that was added when the CA's DN entry in the Directory was created. This
password allows Security Manager to write certificate information to the
```

```
Directory.
> xxxxxxxx

Enter the full DN for the First Officer.
[cn=First Officer,ou=CA,o=Entrust] >

================================================================================
 Directory Administrator
================================================================================

Enter the distinguished name (DN) of the Directory Administrator. Security
Manager Administration requires this to log in to the Directory in order to
perform maintenance tasks such as adding and removing users.
The Directory Administrator's DN may look something like this:
  cn=diradm or
  cn=DirectoryAdministrator,ou=CA,o=Entrust
[cn=diradm] > cn=diradmin,ou=CA,o=Entrust

Enter the password for the Directory Administrator. Use the same password that
was used when the Directory Administrator was created.
> xxxxxxxx

================================================================================
 TCP Communication Ports
================================================================================

Please enter the TCP ports for the Security Manager communications protocols.

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]  :


================================================================================
 CSCA Configuration
================================================================================

Is this a Country Signing CA (CSCA) (y/n) ? [n]

================================================================================
 Algorithms
================================================================================

Are you using a hardware device for the CA keys (y/n) ? [n] y

Enter the pathname for the CryptokiLibrary.
[/opt/nfast/toolkits/pkcs11/libcknfast.so] >

Choose one of:
1. nCipher Corp. Ltd  SN : 03e4674dc52cd093 SLOT : 492971158
> 1

Enter the type of key that Security Manager will use for signing operations.
Select one of the following:
         1. RSA
         2. DSA
         3. EC
[1] >1

Please select RSA type and corresponding key length you wish to use.
Select one of the following:
         1. RSA-1024
         2. RSA-2048
         3. RSA-3072
         4. RSA-4096
         5. RSA-6144
[2] >2

Enter the algorithm that Security Manager will use for signing operations.
Select one of the following:
```

```
         1. RSA-SHA1
         2. RSA-SHA224
         3. RSA-SHA256
         4. RSA-SHA384
         5. RSA-SHA512
         6. RSAPSS-SHA1
         7. RSAPSS-SHA224
         8. RSAPSS-SHA256
         9. RSAPSS-SHA384
         10. RSAPSS-SHA512
[3] >3

Enter the type of key pair that will be used for user signing and
nonrepudiation keys.
Select one of the following:
         1. RSA
         2. DSA
         3. EC
[1] >1

Please select RSA type and corresponding key length you wish to use.
Select one of the following:
         1. RSA-1024
         2. RSA-2048
         3. RSA-3072
         4. RSA-4096
         5. RSA-6144
[2] >2

Enter the type of key pair that will be used for user encryption and dual usage
key pairs.
Select one of the following:
         1. RSA
         2. EC
[1] >1

Please select RSA type and corresponding key length you wish to use.
Select one of the following:
         1. RSA-1024
         2. RSA-2048
         3. RSA-3072
         4. RSA-4096
         5. RSA-6144
[2] >2

================================================================================
 Compatibility With Microsoft (R) Windows (R) Applications
================================================================================

If you choose to work with Microsoft (R) Windows (R) applications, this will
affect how Certificate Revocation Lists (CRLs) are issued after CA key update
and how the CRL Distribution Point (CDP) appears in certificates.

In addition, there are other settings that you must manually configure.  For
more information consult the Security Manager documentation and white papers.

Do you wish to work with Microsoft (R) Windows (R) applications (y/n) ? [n]

================================================================================
 CRL Distribution Points (CDP) and Combined CRL
================================================================================

The default CDP (cRLDistributionPoints) extension URL names can be defined now
or later by editing entmgr.ini.
Enter CDP URL data now (y/n) ? [y] n

================================================================================
 Database Parameters
================================================================================

Creating ODBC inifile '/opt/entrust/authdata/CA/.odbc.ini'...
```

```
Checking PostgreSQL server status ... Server is running.

Enter the password for the database user (easm_entrust) for Security Manager.
>
easm_entrust: Successfully connected to PostgreSQL.
The Entrust schema has already been applied, and contains no data.

Enter the password for the database backup user (easm_entbackup) for Security
Manager.
>
easm_entbackup: Successfully connected to the database.

Enter the algorithm that will be used for database encryption.
Select one of the following:
         1. AES-CBC-128
         2. AES-CBC-256
         3. AES-GCM-128
         4. AES-GCM-256
         5. TRIPLEDES-CBC-192
[2] >

================================================================================
 CA Parameters
================================================================================

A hierarchy of CAs comprises several CAs linked into a tree structure. There is
a single CA which unites the tree into a single structure. This CA is the "Root
CA". A CA which does not participate in a hierarchy is also referred to as a
"Root CA" since it may have subordinates at some time in the future. Any other
CA in the hierarchy is called a "Subordinate CA".

Choose the type of CA you wish to configure.
Select one of the following:
         1. Root CA
         2. Subordinate CA
[1] >1

Is this Root CA a Single Point of Contact (SPOC) CA (y/n) ? [n]

Enter the CA certificate lifetime in months (2-3000) or to Dec 30 2999 23:59:59
UTC, whichever is shorter.
[120] >

Enter the CA private key usage period (20.0000-100.0000).
[100] >

================================================================================
 Policy Certificate Lifetime
================================================================================

Enter the policy certificate lifetime in days (1-3650).
[30] >

================================================================================
 Automatic Login
================================================================================

Automatic login enables service startup without entering a password. It also
allows some Security Manager Control Command Shell commands to be run without a
password.

Do you want to enable automatic login (y/n) ? [n] y

================================================================================
 Security Manager 10.0.1 Configuration Review
================================================================================

1. Directory Comms:         10.194.148.96+389, LDAPv3, Binary
2. CA DNs, CRLs:            ou=CA,o=Entrust; cn=First Officer,ou=CA,o=Entrust
3. Dir Admin:               cn=diradmin,ou=CA,o=Entrust
4. Country Signing CA (CSCA)
```

```
       CSCA:                no
5. Algorithms:
       CA Keys:
                            Signing: RSA-2048 (hardware)
                            SignatureAlg: RSA-SHA256
       User Keys:
                            Encryption: RSA-2048
                            Signing: RSA-2048
6. Security Manager TCP ports:
       PKIX-CMP:            829    Entrust-proto-PKIX:  709
       Admin:               710    XAP:          443
7. CA parameters:
       Type:                Root
       CA Cert Lifetime:    120 (months)
       CA Key Usage Period: 100 %
8. Clients:                 Does not work with Microsoft (R)
                            Windows (R) applications
9. CDP (cRLDistributionPoints extension), Combined CRL:
       Combined CRL:                Enabled

       No CDPs have been defined
10. Database parameters:
       Hostname/IP address: localhost
       Port:                5432
       Database name:       easm_DB
       Database user:       easm_entrust
       Encryption:          AES-CBC-256
11. Policy certificate:      Lifetime: 30 (days)
12. Licensing Information
       Enterprise Serial Number:    entrust
       Enterprise User Limit:       5000
       Enterprise Licensing Code:   JWIP3QAS
       Web Serial Number:           entrust
       Web User Limit:              5000
       Web Licensing Code:          UNTZUKR7
13. Autologin for services and commands:
       Autologin:                   Enabled

Enter section number to review, or enter 'yes' to finish.
[yes] > yes
Created file: /opt/entrust/authdata/CA/manager/entmgr.ini
Created file: /opt/entrust/authdata/CA/manager/initial.certspec
Created file: /opt/entrust/authdata/CA/optional/client_entrust.ini
Created file: /opt/entrust/authdata/CA/manager/entrust.ini
Created file: /opt/entrust/authdata/CA/manager/entDvt.ini
Created file: /opt/entrust/authdata/CA/env_settings.sh
Created file: /opt/entrust/authdata/CA/env_settings.csh
Created file: /opt/entrust/authdata/CA/optional/entrustra.ini

Most configuration problems arise from incorrect Directory settings. It is
recommended that you verify that Security Manager can use the Directory
information that you have entered up to this point. If you would like to verify
the Directory information, first ensure that the Directory is running.
Would you like to verify the Directory information (y/n) ? [y]

Starting the Directory Verification Test...

Initializing test program...
Testing directory configuration...
Performing LDAP v3 Test.
This test may take up to 1 minute to complete.
Performing Client Test.
Performing CA Credentials Test.
Performing Diradmin Credentials Test.
Performing CA Entry Schema Test.
Performing CA Entry CA Certificate Test.
Performing CA Entry CRL Test.
Performing CA Entry Cross-Certificate Pair Test.
Performing CA Entry Policy Certificate Test.
Performing CRL Distribution Point Test.
Performing Policy Certificate Distribution Point Test.
```

```
Performing First Officer Test.
Performing ASH Entry Test.
Performing Diradmin Test.
Performing Multi-Attribute RDN Test.
Directory testing complete with no notes or errors detected.

Checking PostgreSQL server status ... Server is running.
Stopping PostgreSQL Database server...
Server stopped.
Starting PostgreSQL Database server...
PostgreSQL Database server started.

If you want to use a customized certificate specifications file instead of the
default certificate specifications file, you can provide the full path to the
customized file. The default certificate specifications file at
'/opt/entrust/authdata/CA/manager/initial.certspec' will be renamed to
'initial.certspec.default', and 'initial.certspec' will be a copy of your
customized file.
Enter the full path of your customized certificate specifications file, or
press Enter to use the default.
>

Would you like to perform the first time initialization and start the CA now?
If you need to customize any settings in entmgr.ini or initial.certspec, you
should exit now and follow the procedures in the documentation.
Select one of the following:
     1. Initialize CA using Security Manager Control Command Shell
     2. Exit (do not initialize the CA now)
> 1

executing /opt/entrust/authority/bin/entsh -e "source
"/opt/entrust/authdata/CA/FirstTimeInit.tcl""
Starting first time initialization...

A Hardware Security Module (HSM) will be used for the CA key:
    nCipher Corp. Ltd  SN : 4dc9b4a2e2343d37
    The HSM requires a password.

Enter password for CA hardware security module (HSM):
Enter new password for Master1:
Confirm new password for Master1:
Enter new password for Master2:
Confirm new password for Master2:
Enter new password for Master3:
Confirm new password for Master3:
Enter new password for First Officer:
Confirm new password for First Officer:

Initialization starting; creating ca keys...
Initialization complete.
Starting the services...
Creating CA profile...
Creating First Officer profile...
You are logged in to Security Manager Control Command Shell.
Performing database backup...
NOTICE:  pg_stop_backup complete, all required WAL segments have been archived
SUCCESS: Full backup completed successfully.
Press return to exit
```

2.11. Initialize Security Manager

1. Open a command prompt and log in as `Master1`.
2. Source the environment setting file:

```
# source /opt/entrust/authdata/CA/env_settings.sh
```

3. Run the initialization script:

```
# entsh -e "source /opt/entrust/authdata/CA/FirstTimeInit.tcl"
```

2.12. Launch a Security Manager Shell

1. Open a command prompt and log in as `Master1`.
2. Source the environment setting file:

```
# source /opt/entrust/authdata/CA/env_settings.sh
```

3. Open an Entrust Shell.

```
# entsh
```

Further commands during testing are executed inside the Entrust shell.

2.13. Show the Security Manager status

Open a Security Manager shell as described above and type the following command. It may take several minutes for all the services to be up.

```
entsh$ service status
Checking service status...
amb     Maintenance               enabled  up  1 processes
ash     Admin Service Handler     enabled  up  4 processes
backup  Automatic Backup          enabled  up  1 processes
cmp     PKIX-CMP                  enabled  up  2 processes
integ   Database Integrity Check  enabled  up  1 processes
keygen  Key Generator             enabled  up  1 processes
listen  Listener Service          enabled  up  1 processes
rlsvc   Revocation List Service   enabled  up  1 processes
sep     Entrust proto-PKIX        enabled  up  2 processes
xap     XML Admin Protocol        enabled  up  2 processes
```

2.14. Show the HSM status

Open a Security Manager shell and type the following command.

```
entsh$ ca key show-cahw
You must log in to issue the command.
Master User Name: Master1
Password:

**** Hardware Information ****

-----------------------------------------------------

Name:
nCipher Corp. Ltd  SN : 201f114b435dbe89 SLOT : 761406613

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
ECDSA style:              4 (use raw digest padded to large digest size)

-----------------------------------------------------
**** End of Hardware Information ****
```

2.15. Import key from the Entrust Security Manager database to the HSM

Open a Security Manager shell and type the following command.

Select **nCipher Corp. Ltd SN :...** when prompted for **Select the destination for the new CA key**.

```
entsh$ ca key update
You must log in to issue the command.
Master User Name: Master1
Password:

Select the destination for the new CA key.
Choose one of:
1. Software
2. nCipher Corp. Ltd  SN : 201f114b435dbe89 SLOT : 761406613
3. Cancel operation
> 2
Checking cluster status...

100% complete. Estimated time remaining -:-:- |

CA key and certificate successfully updated.
Recovering CA profile...

CA profile successfully recovered.

It is recommended that all revocation lists be re-issued. This can be done
later with the 'rl issue' command. Re-issue revocation lists now (y/n) ? [y]

Issuing CRLs, please wait ...


1 CRL(s) were issued.
1 ARL(s) were issued.
1 combined CRL(s) were issued.



Publishing CRLs, please wait ...

ou=CA,o=Entrust.Master1 $
```

2.16. Export the key from the HSM to the Entrust Security Manager database

Open a Security Manager shell and type the following command.

Select **Software** when prompted for **Select the destination for the new CA key**.

```
entsh$ ca key update
```

2.17. List all the keys

Open a Security Manager shell and type the following command.

Notice keys in both the Security Manager database and the HSM as indicated by the *hardware status" parameter below.

```
entsh$ ca key show-cache
**** In Memory CA cache ****
Record Status Legend:
  C = current key
  H = key on hold
  A = non-current key
  X = revoked or expired non-current key has been obsoleted
  HWV1 = hardware key PKCS11 V1 *** NOT SUPPORTED ***
  HWV2 = hardware key PKCS11 V2
  SW = software key

-----------------------------------------------------

Internal key index:           1
CA certificate issued by:     ou=CA,o=Entrust
serial number:                00D6070404F791619D38DFA7D824CAC117
current CA certificate:       N
CA certificate issue date:    Mon Dec  6 21:14:51 2021
CA certificate expire date:   Sat Dec  6 21:44:51 2031
subject key identifier:       3B2E0E1264722E192605E59EDE32864B117175C7
private key active:           Y
private key expired:          N
certificate expired:          N
certificate revoked:          N
revocation details:           N/A
key:                          RSA-2048
global signing policy:        RSA-SHA256 (sha256WithRSAEncryption)
record status in database:    A HWV2
migrated:                     N
hardware load error:          N
hardware CKA_ID:              2nh+mYAJJfEDjMy+SynUmhzmN7g=
hardware status: Loaded >> 'nCipher Corp. Ltd  SN : 201f114b435dbe89 SLOT : 761406613'.

-----------------------------------------------------

Internal key index:           2
CA certificate issued by:     ou=CA,o=Entrust
serial number:                0DEB0B5DBC9D151903EEB23A8AB18510
current CA certificate:       N
CA certificate issue date:    Tue Dec  7 15:33:08 2021
CA certificate expire date:   Sun Dec  7 16:03:08 2031
subject key identifier:       FC5FADA60FFC265C30071C84983B37A16201444A
private key active:           Y
private key expired:          N
certificate expired:          N
certificate revoked:          N
revocation details:           N/A
key:                          RSA-2048
global signing policy:        RSA-SHA256 (sha256WithRSAEncryption)
record status in database:    A SW
migrated:                     N
hardware load error:          N
hardware CKA_ID:              N/A
hardware status: CA Hardware not used.

...

-----------------------------------------------------
**** End of In Memory CA cache ****
```

2.18. List all the certificates

Open a Security Manager shell and type the following command.

```
entsh$ ca cert list
You must log in to issue the command.
Master User Name: Master1
Password:
Serial Type    Issue Date           Expiry Date          Post  Revoked
[1]    CA      2021/12/06 21:14:51  2031/12/06 21:44:51  yes
[2]    CA      2021/12/07 15:33:08  2031/12/07 16:03:08  yes
[3]    LINK    2021/12/06 21:14:51  2031/12/06 21:44:51  yes
[4]    LINK    2021/12/07 15:33:08  2031/12/06 21:44:51  yes
[5]    CA      2021/12/07 15:39:53  2031/12/07 16:09:53  yes
[6]    LINK    2021/12/07 15:33:08  2031/12/07 16:03:08  yes
[7]    LINK    2021/12/07 15:39:53  2031/12/07 16:03:08  yes
[8]    CA      2021/12/07 15:49:20  2031/12/07 16:19:20  yes
[9]    LINK    2021/12/07 15:39:53  2031/12/07 16:09:53  yes
[10]   LINK    2021/12/07 15:49:20  2031/12/07 16:09:53  yes

The certificate with serial number [8] is the current CA certificate.

Serial Numbers:
[1] 00D6070404F791619D38DFA7D824CAC117
[2] 0DEB0B5DBC9D151903EEB23A8AB18510
[3] 31E0445429936E9A52DC92D2EE11B872
[4] 35C1FB5035EE175B31C76CE441311BDC
[5] 3201312D8A6C37B67F15FAB2C8865BDA
[6] 537FCA725616E8B573EFD49F400D7A0D
[7] 00C4E5BD16480FD06AFF8FE6937B78A959
[8] 6FD12E2901D19F2AB9220A67F6FB1E83
[9] 00EACB54949E07A722D1877AC1E640FB19
[10] 0091A503A442D00BC8A53527CA5648A5C4


ou=CA,o=Entrust.Master1 $
```

2.19. Back up Security World files

1. Back up the `/opt/nfast/kmdata/local` directory.

   Such a backup of Security World files must be performed after any new key generation or Security World administration activities.

2. Store the backup files according to your organization's disaster recovery instructions.

3. Troubleshooting

The following are error messages that might appear during the procedures described in this guide.

3.1. (-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$`).

Resolution

1. Open the Master Control shell (`entsh$`):
2. Log in with `Master1`.
3. Run `Service Start`.

3.2. ./config_authority.sh fails to detect the PKCS11 library

Script is checking if there is execute permissions on libcknfast.so.

Resolution

Give execute permissions to `/opt/nfast/toolkits/pkcs11/libcknfast.so`.

```
% chmod +x /opt/nfast/toolkits/pkcs11/libcknfast.so
```

3.3. Error encountered querying CA hardware

When you are configuring Security Manager, you see the following message:

```
Are you using a hardware device for the CA keys (y/n) ? [n] y

Enter the pathname for the CryptokiLibrary.
[/opt/nfast/toolkits/pkcs11/libcknfast.so] >

Error encountered querying CA hardware.
```

Resolution

Make sure you have an OCS card in the HSM. What the card is in place, the script should be able to see the HSM.

3.4. (-77) Problem reported with crypto hardware.

When initializing Entrust SM, you see the following message:

```
Initialization starting; creating ca keys...
(-77) Problem reported with crypto hardware.
GenerateKeyPairX509
Press return to exit
```

Resolution

Make sure that the following variable in `cnkfastrc` is set to `1`.

```
CKNFAST_LOADSHARING=1
```

3.5. cannot initialize: Current Unix user does not have proper group membership to access Security Manager.

When initializing Entrust SM, you see the following message:

```
Starting first time initialization...
!StartMgrProc(es): (1) Operation not permitted @ src/manager/mush/Mush.cpp.351
cannot initialize: Current Unix user does not have proper group membership to access Security Manager.
(1) Operation not permitted
Press return to exit
```

Resolution

Make sure the `Master1` primary group is `easm_entrust_pg`:

```
sudo usermod -g easm_entrust_pg Master1
```

3.6. HSM logs show missing algorithms errors that are not configured by Security Manager during startup

Security Manager performs a FIPS self-test. This includes many algorithms and functions beyond those explicitly configured to be used once operational. These tests are required by FIPS 140-x conformance.

Resolution

- Security Manager treats any algorithm that is not available during self-test as for information only.
- FIPS Self Tests HSM log errors do *not* stop the Security Manager startup.

3.7. No Hardware Device Found

During the configuration of Security Manager, the message **No Hardware Device Found** appears every time, even if the correct library is selected.

Resolution

- Make sure that `entconfig.ini` and `entrust.ini` both have the correct PKCS #11 library setting.
- Ensure that any HSM service is running.

3.8. (-2684) General hardware error

HSM Service is not available.

Resolution

Ensure that any HSM service is running and responding.

3.9. Database backup failed during the Entrust Security Manager configuration

Another symptom is "walfile failed to appear". Refer to technote https://trustedcare.entrust.com/articles/en_US/Technote/DB-Backup-Fails.

Resolution

1. Edit the **archive_command** parameter in the following files as described above.

   `/var/pgsql/easm_entrust_pg_data_11/postgresql.conf`
   `/opt/entrust/easm_postgresql_11.7/etc/postgresql.conf`

2. Ensure the correct ownership of these files:

```
# chown easm_entrust_pg:easm_entrust_pg /var/pgsql/easm_entrust_pg_data_11/postgresql.conf

# chown easm_entrust_pg:easm_entrust_pg /opt/entrust/easm_postgresql_11.7/etc/postgresql.conf
```

3.10. Security Manager configuration fails

This procedure also applies when switching HSMs.

Resolution

1. Removed older configuration data:

```
# sudo rm -rf /opt/entrust/authdata
```

2. Uninstall and re-install the PostgreSQL database as described in section **Install the Entrust Authority database**.
3. Redo the Security Manager configuration as described in section **Configure the Entrust Security Manager**.