Entrust Certificate Authority

nShield® HSM Integration Guide for Linux

2025-02-07

Table of Contents

1. Introduction . . . 1
    1.1. Product configuration . . . 1
    1.2. Supported nShield hardware and software versions . . . 1
    1.3. Requirements . . . 2
2. Install and configure directory service . . . 3
    2.1. Install directory service . . . 3
    2.2. Configure directory service . . . 3
3. Install and configure the Entrust nShield HSM . . . 5
    3.1. Select the protection method . . . 5
    3.2. Install the HSM . . . 5
    3.3. Install the nShield Security World Software and create the Security World . . . 6
    3.4. Create the OCS or Softcard in the CA server . . . 6
4. Install the Entrust Certificate Authority . . . 9
    4.1. Install the Entrust Authority database . . . 9
    4.2. Create Master Users . . . 10
    4.3. Install the Entrust Certificate Authority . . . 11
5. Configure the Entrust Certificate Authority . . . 13
    5.1. Establish a preload session . . . 13
    5.2. nShield Edge pre-configuration . . . 15
    5.3. Configure the Entrust Certificate Authority . . . 15
6. Test the integration . . . 30
    6.1. Initialize Entrust Certificate Authority . . . 30
    6.2. Launch an Entrust Certificate Authority shell . . . 30
    6.3. Show the Entrust Certificate Authority status . . . 31
    6.4. Show the Entrust nShield HSM status . . . 31
    6.5. Import a key from the Entrust Certificate Authority database . . . 32
    6.6. Export the key from the nShield HSM to the Entrust Certificate Authority database . . . 33
    6.7. List all keys . . . 34
    6.8. List all certificates . . . 35
    6.9. Back up Entrust nShield HSM Security World files . . . 36
7. Troubleshooting . . . 37
    7.1. (-8973) Could not connect to the Entrust Certificate Authority service. Certificate Authority service may not be running . . . 37
    7.2. ./config_authority.sh fails to detect the PKCS11 library . . . 37
    7.3. Error encountered querying CA hardware . . . 38

7.4. (-77) Problem reported with crypto hardware . . . 38
7.5. Cannot initialize: Current Unix user does not have proper group membership to access Certificate Authority . . . 38
7.6. HSM logs show missing algorithms errors that are not configured by Certificate Authority during startup . . . 39
7.7. No Hardware Device Found . . . 39
7.8. (-2684) General hardware error . . . 39
7.9. Database backup failed during the Entrust Certificate Authority configuration . . . 40
7.10. Certificate Authority configuration fails . . . 40
7.11. nShield Edge Cluster Status . . . 41
8. Additional resources and related products . . . 42
8.1. nShield Connect . . . 42
8.2. nShield as a Service . . . 42
8.3. nShield Edge . . . 42
8.4. Entrust products . . . 42
8.5. nShield product documentation . . . 42

Chapter 1. Introduction

The Entrust Certificate Authority 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 nShield as a Service (nSaaS). 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 Certificate Authority	v10.2.1
PostgreSQL	v15.2.1
Red Hat Enterprise Server	v8.0

1.2. Supported nShield hardware and software versions

Entrust successfully tested with several nShield hardware and software versions.

Module-protected keys are not supported in Entrust Security Manager v10.0 and later versions. OCS and softcard protection was tested in all configurations.

Product	Security World Software	Firmware	Netimage
nSaaS	13.4.5	12.72.1 (FIPS 140-2 certified)	12.80.5
nShield Edge	13.4.5	12.72.0 (FIPS 140-2 certified)	

Product	Security World Software	Firmware	Netimage
nShield Solo XC	13.4.5	12.72.1 (FIPS 140-2 certified)	
Connect XC	13.6.3	12.72.1 (FIPS 140-2 certified)	12.80.5
nShield 5s	13.6.3	13.4.5 (FIPS 140-3 Certified)	
nShield 5c	13.6.3	13.4.5 (FIPS 140-3 Certified)	13.6.5

1.3. Requirements

To integrate the HSM and Certificate Authority, you require:

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

Familiarize yourself with:

- The Entrust Certificate Authority (https://www.entrust.com/digital-security).
- The nShield HSM: *Installation Guide* and *User Guide*.
- Your organizational Certificate Policy, 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 Level 3.
  - Key attributes such as key size, time-out, or needed for auditing key usage.

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Install and configure directory service

Installation and configuration steps:

1. Install directory service
2. Configure directory service

2.1. Install directory service

The Entrust Certificate Authority requires an LDAP (Lightweight Directory Access Protocol) compliant directory service or a third-party LDAP-compliant X.500 directory. A remote OpenLDAP directory service with a self-signed certificate was used in this integration. See PSIC-Entrust Certificate Authority x for the list of directory services supported.

1. Install the required directory service.
2. Add the following firewall rule if accessing a directory in another server:

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

2.2. Configure directory service

The Entrust Certificate Authority directory schema configuration is described in Entrust Certificate Authority 10.0 Documentation Suite - Issue x.

1. Implement the configuration corresponding to your directory service.

   The following directory service parameters are used in this integration:

   - Top Level DN: `dc=entrustsm,dc=local`
   - CA Directory Location: `ou=CAentry,dc=entrustsm,dc=local`
   - Director Administrator: `cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local`
   - First Officer: `cn=FirstOfficer,ou=CAentry,dc=entrustsm,dc=local`

2. Test access to the directory services:

```
[root@entrust-sm-linux ~]# ldapsearch -x -H ldap://<Name_or_IP> -D
"cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -b "cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -s
sub -W
Enter LDAP Password:
# extended LDIF
```

```
#
# LDAPv3
# base <cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# EntrustAdmin, CAentry, entrustsm.local
dn: cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: entrustadmin
sn: Administrator
userPassword:: e1NTSEF9dll6U0huV2w3Wm90MFJPTTFDbVhzVjIycHhyckkvREw=
description: Certificate Authority Directory Administrator
cn: EntrustAdmin

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Chapter 3. Install and configure the Entrust nShield HSM

Installation and configuration steps:

1. Select the protection method
2. Install the HSM
3. Install the nShield Security World Software and create the Security World
4. Create the OCS or Softcard in the CA server

3.1. Select the protection method

OCS, Softcard, or Module protection can be used to authorize access to the keys protected by the HSM. When selecting your protection method take into consideration:

- Your organization's security policy.
- Unattended startup requirements.

The OCS or Softcard needs to the presented initially when configuring the Entrust Certificate Authority. In production, unattended startup is possible in some scenarios.

3.2. 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:

- How to locally set up a new or replacement nShield Connect
- How to remotely set up a new or replacement nShield Connect
- How to remotely set up a new or replacement nShield Connect XC Serial Console model

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

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

To 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. Open a command window and 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
 ...
```

5. 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.

6. Confirm the Security World is `usable`:

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

3.4. Create the OCS 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.

3.4.1. Create the OCS

To 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 an administrator.
3. Run the `createocs` command as described below, entering a passphrase or password at the prompt.

   Create one card for each person with access privilege, plus the spares. In this guide, the quorum K equal and total numbers of cards N is set to 1 for simplicity.

   The **--persist** option allows for removal of the OCS for save storage. Otherwise, the authentication provided by the OCS is only available while the OCS card is inserted in the HSM front panel slot, or the TVD. Notice `slot 2`, remote via a Trusted Verification Device (TVD), is used to present the card.

   

   After an Operator Card Set has been created, the cards cannot be duplicated.

```
# createocs -m1 -s2 -N testOCS -Q 1/1 --persist

FIPS 140-2 level 3 auth obtained.

Creating Cardset:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: Admin Card #5
 Module 1 slot 2: blank card
 Module 1 slot 3: empty
 Module 1 slot 4: empty
 Module 1 slot 5: empty
 Module 1 slot 2:- passphrase specified - writing card
Card writing complete.

cardset created; hkltu = edb3d45a28e5a6b22b033684ce589d9e198272c2
```

4. Verify the OCS was created:

```
# nfkminfo -c
Cardset list - 2 cardsets:  (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
 Operator logical token hash               k/n timeout  name
 edb3d45a28e5a6b22b033684ce589d9e198272c2  1/5  none-NL testOCS
```

   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 testOCS                 0 (0)        1 of 5; persistent
rocs> quit
```

3.4.2. Create a Softcard

To create a Softcard:

1. Run the following command and enter a passphrase or password at the prompt:

```
# ppmk -n testSC

Enter new pass phrase:
Enter new pass phrase again:
New softcard created: HKLTU 925f67e72ea3c354cae4e6797bde3753d24e7744
```

2. Verify the Softcard was created:

```
# nfkminfo -s
SoftCard summary - 1 softcards:
 Operator logical token hash               name
 925f67e72ea3c354cae4e6797bde3753d24e7744  testSC
```

   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 testOCS                 0 (0)        1 of 1; persistent
  2 testSC                  0 (0)        (softcard)
rocs>
```

Chapter 4. Install the Entrust Certificate Authority

Steps:

1. Install the Entrust Authority database
2. Create Master Users
3. Install the Entrust Certificate Authority

4.1. Install the Entrust Authority database

Entrust Certificate Authority 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 Certificate Authority 10.0* on Entrust TrustedCare.

An embedded Certificate Authority PostgreSQL database is used for the purposes of this guide. This database will be installed on the same server that will host Certificate Authority.

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 *Certificate Authority Database Configuration Guide*.

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

1. Download the PostgreSQL Server file `Entrust-Certificate-Authority-PostgreSQL-15-15.2.10-25.el8.x86_64.rpm` from the Entrust TrustedCare online support site https://trustedcare.entrust.com/MyProductsList. Under **PKI**, expand **Authority**. Then select the **Certificate Authority** version. The PostgreSQL Server file is listed among the available downloads.
2. Install dependencies:

   ```
   % dnf install compat-openssl10.x86_64
   ```

3. Navigate to the directory where you downloaded the rpm file to and start the installation:

```
% cd Downloads
% rpm -i Entrust-Certificate-Authority-PostgreSQL-15-15.2.10-25.el8.x86_64.rpm
```

4. Run the PostgreSQL setup script

```
% cd /opt/entrust/easm_postgresql_15/dbserver/bin
% ./setup_easm_DB.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.

4.2. Create Master Users

Master Users are responsible for controlling the Entrust Certificate Authority software through the Certificate Authority 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 Certificate Authority, so they can choose and enter their own unique and private passwords. Also, they must have physical access to the server that hosts Certificate Authority, so that they can maintain the Certificate Authority infrastructure.

Master Users use Certificate Authority Control Command Shell to:

- Start and stop the Certificate Authority service.
- Back up and restore the Certificate Authority 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 Certificate Authority PostgreSQL Database installer creates the `easm_entrust_pg` group.

Certificate Authority, previously known as Security Manager, in older versions might require an entrust group be created as such:

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

To create Master Users:

1. 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
```

2. Add users to groups:

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

3. Set the users passwords:

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

4.3. Install the Entrust Certificate Authority

To install the Entrust Certificate Authority:

1. Download Certificate Authority for Linux `Entrust-Certificate-Authority-10.1.1-1543.el8.x86_64.rpm` from the Entrust TrustedCare online support site.
2. Install dependencies:

```
% yum install libnsl
```

3. Run the installer. Use the **-e** option first to remove the current installation. Then use the **-U** option to reinstall. This applies whether upgrading an older version, or simply reinstalling the same version. Use the **-i** option for a new installation.

```
# rpm -i /root/Downloads/Entrust-Certificate-Authority-10.1.1-1543.el8.x86_64.rpm
warning: /root/Downloads/security-manager-10.0.31-3.el8.x86_64.rpm: Header V4 RSA/SHA256 Signature, key ID
ac33653e: NOKEY
   Verifying OS support...
   OS is a supported OS.
   Found PG user home directory [/home/easm_entrust_pg]
   Updating /etc/sudoers.d/securitymanager...
%easm_entrust_pg ALL=(easm_entrust_pg) NOPASSWD: /usr/bin/zip
%easm_entrust_pg ALL=(easm_entrust_pg) NOPASSWD: /home/easm_entrust_pg/sm_pg_initd.sh
   Updating archiving settings in /var/pgsql/easm_entrust_pg_data_11/postgresql.conf
   Updated archive settings in /var/pgsql/easm_entrust_pg_data_11/postgresql.conf.
#
```

Chapter 5. Configure the Entrust Certificate Authority

Steps:

1. Establish a preload session
2. nShield Edge pre-configuration
3. Configure the Entrust Certificate Authority

5.1. Establish a preload session

The OCS or the Softcard must be preloaded to configure the Certificate Authority.

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 environment variable pointing to the location of the file created above. In addition, add the other variables shown below. The PCKS11 #11 log variables are optional.

```
# cat /opt/nfast/cknfastrc

# Softcard
CKNFAST_LOADSHARING=1

# Other variables
CKNFAST_NO_UNWRAP=1
CKNFAST_FAKE_ACCELERATOR_LOGIN=1
CKNFAST_NO_ACCELERATOR_SLOTS=1
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none

# Preload file location
NFAST_NFKM_TOKENSFILE=/opt/nfast/entrustsmtoken

# PCKS #11 log level and file location
CKNFAST_DEBUG=10
CKNFAST_DEBUGFILE=/opt/nfast/log/pkcs11.log
```

   

   When you are using nShield with ePassport CVCA, add the variable `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.

3. Restart the hardserver:

```
# /opt/nfast/sbin/init.d-ncipher restart
```

4. Open a separate command window and preload the Card Set:

   - The `preload -c` command for OCS.
   - The `preload -s` command for Softcard.

> Do not close this window throughout the Entrust Certificate Authority configuration. Otherwise the configuration will fail.

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

Present the OCS cards and passphrase when prompted. For example:

```
# preload -c testOCS -f /opt/nfast/entrustsmtoken pause
2023-02-15 16:21:16: [250942]: INFO: Preload running with: -c testOCS -f /opt/nfast/entrustsmtoken pause
2023-02-15 16:21:16: [250942]: INFO: Created a (new) connection to Hardserver
2023-02-15 16:21:16: [250942]: INFO: Modules newly usable: [1].
2023-02-15 16:21:16: [250942]: INFO: Found a change in the system: an update pass is needed.
2023-02-15 16:21:16: [250942]: INFO: Loading cardset: testOCS in modules: [1]

Loading `testOCS':
 Module 1 slot 0: Admin Card #1
 Module 1 slot 2: empty
 Module 1 slot 3: empty
 Module 1 slot 4: empty
 Module 1 slot 5: empty
 Module 1 slot 2: `testOCS' #1
 Module 1 slot 2:- passphrase supplied - reading card
Card reading complete.

2023-02-15 16:22:01: [250942]: INFO: Stored Admin key: kfips (4c0b...) in module #1
2023-02-15 16:22:01: [250942]: INFO: Loading cardset: Cardset: testOCS (a165...) in module: 1
2023-02-15 16:22:01: [250942]: INFO: Stored Cardset: testOCS (a165...) in module #1
2023-02-15 16:22:01: [250942]: INFO: Maintaining the cardset testOCS protected key(s)=[].
2023-02-15 16:22:01: [250942]: 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 running the following command back on the main window.

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

For example:

```
# preload -c testOCS -f /opt/nfast/entrustsmtoken nfkminfo
2023-10-17 16:48:09: [201880]: INFO: Preload running with: -c testOCS -f /opt/nfast/entrustsmtoken nfkminfo
2023-10-17 16:48:09: [201880]: INFO: Created a (new) connection to Hardserver
2023-10-17 16:48:09: [201880]: INFO: Modules newly usable: [1].
2023-10-17 16:48:09: [201880]: INFO: Found a change in the system: an update pass is needed.
2023-10-17 16:48:10: [201880]: INFO: Maintaining the cardset testOCS protected key(s)=[].
2023-10-17 16:48:10: [201880]: INFO: Loading complete. Executing subprocess nfkminfo
World
 generation  2
 state       0x373f000c Initialised Usable Recovery !PINRecovery ExistingClient RTC NVRAM FTO
AlwaysUseStrongPrimes !DisablePKCS1Padding !PpStrengthCheck !AuditLogging SEEDebug AdminAuthRequired

 ...

Pre-Loaded Objects (  2):  objecthash   module objectid  generation
 edb3d45a28e5a6b22b033684ce589d9e198272c2   1 0x80a93202 1
 003e04e3c07fb5791f651c992da5527779159f87   1 0x80a93201 1
```

5.2. nShield Edge pre-configuration

The nShield Edge exhibits slower service startup times with respect to operations, which is to be expected. If you are using an nShield Edge device, you must adjust the `.ini` file settings for Certificate Authority. This enables a sufficient timeout duration for the system to initialize properly:

1. Navigate to the `ini` directory. By default, this is `/opt/entrust/authority/etc/ini/entMgr.ini`.
2. Edit the `entMgr.ini` file, locate the **[login]** section, and add the following settings:

```
serviceStartStopWaitSeconds=3600
clusterStartWaitSeconds=1800
clusterStopWaitSeconds=300
```

For more information regarding these settings, refer to *Certificate Authority 10.0 Configuration File Management Guide Issue 5.0*, which is available on the Entrust TrustedCare Portal.

5.3. Configure the Entrust Certificate Authority

The Entrust Certificate Authority configuration is an interactive process to choose

certificate algorithms, lifetimes, and other options for your Certification Authority.

1. Preload the OCS or Softcard as described in Establish a preload session if you have not yet done so.
2. Install the OpenLDAP client if you have not yet done so.
3. Make the PCKS11 cryptographical library executable by all:

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

4. Give all permissions to the kmdata/local folder

```
# chmod 777 /opt/nfast/kmdata/local
```

5. If logging PKCS #11 as defined in `/opt/nfast/cknfastrc`, create the following file:

```
# sudo touch /opt/nfast/log/pkcs11.log
# sudo chmod 777 /opt/nfast/log/pkcs11.log
```

6. Test access to the directory service from the Certificate Authority server:

```
# ldapsearch -x -H ldap://<Name_or_IP> -D "cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -b
"cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -s sub -W
```

7. Make sure you are root user

```
# su
```

8. Navigate to the Certificate Authority's `\bin` directory:

```
# cd /opt/entrust/certificate_authority/bin
```

9. Invoke the configuration shell script. Enter the information required when prompted as described in the table below.

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.

If the configuration fails after all, do as described in Certificate Authority configuration fails.

```
# ./config_authority.sh
```

Prompt	Value
Enter the required database deployment model.	**embedded**
Enter the installation directory for Certificate Authority CA data (`authdata`)	Select **Enter** to accept default value
Enter the full path of the CA data directory	Select **Enter** to accept default value
Enter the Enterprise licensing information that appears on your Entrust licensing card	Enter Serial Number, Enterprise User Limit, and Enterprise Licensing Code
Enter the Web licensing information that appears on your Entrust licensing card	Enter Web Serial Number, Web User Limit, and Web Licensing Code
Enter the CVCA licensing information for domestic DVs that appears on your Entrust licensing card	Enter the Domestic DV Serial Number or **Enter**
Enter the CVCA licensing information for foreign DVs that appears on your Entrust licensing card.	Enter the Foreign DV Serial Number or **Enter**
Enter the DV licensing information for Inspection Systems that appears on your Entrust licensing card	Enter the IS Serial Number or **Enter**
Enter the type of Directory service	**LDAP Directory** (default)
Enter the hostname or IP address of the machine that is hosting your Directory service	Enter hostname or IP
Enter the Directory TCP port number	**389** (default)

Prompt	Value
Enter the distinguished name (DN) of your Certification Authority (CA)	ou=CAentry,dc=entrustsm,dc=local
Enter the password for this Certification Authority (CA).	Enter password
Enter the full DN for the First Officer	cn=FirstOfficer,ou=CAentry,dc=entrustsm,dc=local
Enter the distinguished name (DN) of the Directory Administrator	cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local
Enter the password for the Directory Administrator	Enter password
Please enter the TCP ports for the Certificate Authority communications protocols	Select **Enter** to accept all defaults: Entrust Proto-PKIX (PKIX) port [709], Entrust Administration Protocol (ASH) port [710], Certificate Management Protocol (PKIX-CMP) port [829], and Entrust XML Administration Protocol (XAP) port [443]:
Is this a Country Signing CA (CSCA) (y/n) ? [n]	**n** (default)
Are you using a hardware device for the CA keys (y/n) ? [n]	**y**
Enter the pathname for the Cryptoki Library	`/opt/nfast/toolkits/pkcs11/libcknfast.so`
Choose one of:	**nCipher Corp. Ltd SN : ...**
Enter the type of key that Certificate Authority will use for signing operations	**RSA** (default)
Please select RSA type and corresponding key length you wish to use	**RSA-2048** (default)

Prompt	Value
Enter the algorithm that Certificate Authority will use for signing operations	**RSA-SHA256** (default)
Enter the type of key pair that will be used for user signing and nonrepudiation keys	**RSA** (default)
Please select RSA type and corresponding key length you wish to use	**RSA-2048** (default)
Enter the type of key pair that will be used for user encryption and dual usage key pairs	**RSA** (default)
Please select RSA type and corresponding key length you wish to use	**RSA-2048** (default)
Do you wish to work with Microsoft ® Windows ® applications? (y/n) ? [n]	**n** (default)
Enter CDP URL data now (y/n) ? [y]	**n**
Enter the password for the database user (easm_entrust) for Certificate Authority	Enter password.
Enter the password for the database backup user (easm_entbackup) for Certificate Authority	Enter password.
Enter the algorithm that will be used for database encryption	**AES-CBC-256** (default)
Choose the type of CA you wish to configure	**Root CA** (default)
Is this Root CA a Single Point of Contact (SPOC) CA (y/n) ? [n]	**n** (default)

Prompt	Value
Enter the CA certificate lifetime in months (2-3000)	**120** (default)
Enter the CA private key usage period (20.0000-100.0000)	**100** (default)
Enter the policy certificate lifetime in days (1-3650).	**30** (default)
Do you want to enable automatic login (y/n) ? [n]	**y**
Enter section number to review, or enter 'yes' to finish	Enter number of item to change. Otherwise enter **yes**.
Would you like to verify the Directory information (y/n) ? [y]	**y** (default)
Enter the full path of your customized certificate specifications file, or press Enter to use the default	Select **Enter** to accept default value
Would you like to perform the first time initialization and start the CA now?	**Initialize CA using Certificate Authority Control Command Shell**
Enter password for CA hardware security module (HSM):	Enter the OCS or Softcard passphrase
Enter new password for Master1, Master2, Master3, and First Officer	Enter password

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

```
[Master1@entrust-sm-linux bin]$ ./config_authority.sh


================================================================================
 Entrust Certificate Authority 10.1.1 Configuration
================================================================================

Entrust Certificate Authority Configuration log file: /root/log/config_authority.10.1.1.log

================================================================================
 OS group name
================================================================================
```

```
Entrust Certificate Authority requires that the authdata directory (which
contains CA data) be owned by a dedicated OS group. Please enter the name of
this OS group now. If you have not created the OS group yet, it will be created
at this time.
[eca] >

Looking for OS group [eca]...
   OS group [eca] found.

================================================================================
 OS user name
================================================================================


Entrust Certificate Authority requires that the authdata directory (which
contains CA data) be owned by a dedicated OS user. Please enter the name of
this OS user now. If you have not created the OS user yet, it will be created
at this time.
[eca] >

Looking for OS user [eca]...
   OS user [eca] found.

================================================================================
 easm_entrust_pg group check
================================================================================


Checking for OS user [eca] in OS group [easm_entrust_pg]...
   OS user [eca] is in OS group [easm_entrust_pg].

================================================================================
 /opt/entrust permission check
================================================================================


Checking /opt/entrust permissions for OS user [eca]...
   /opt/entrust writable by OS user [eca].

================================================================================
 Main configuration
================================================================================



Entrust Certificate Authority Configuration log file: /var/tmp/config_authority.10.1.1.log

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/eca_pg_data/15,
PGWAL=/var/pgsql/eca_pg_wal/15, PGDIR=/opt/entrust/easm_postgresql_15.
Detected an existing installation of Entrust Certificate Authority PostgreSQL
```

```
Database on this host.

Enter the desired database deployment model.
Select one of the following:
         1. embedded
         2. customer-supplied
> 1
Checking existing PG version...
You have PostgreSQL database version 11.7 installed.

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

By default, the Certificate Authority 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 Certificate Authority 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:              xxxxxxxx
Enterprise User Limit:      xxxxxxxx
Enterprise Licensing Code:  xxxxxxxx



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 Certificate Authority Administration.
Web Serial Number:          xxxxxxxx
Web User Limit:             xxxxxxxx
Web Licensing Code:         xxxxxxxx



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] >


Enter the hostname or IP address of the machine that is hosting your Directory
service.
[entrust-sm-linux] > 10.194.148.84

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 Certificate Authority 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=CAentry,dc=entrustsm,dc=local

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 Certificate Authority to write certificate information to the
Directory.
>

Enter the full DN for the First Officer.
[cn=First Officer,ou=CAentry,dc=entrustsm,dc=local] > cn=FirstOfficer,ou=CAentry,dc=entrustsm,dc=local

================================================================================
 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=CAentry,dc=entrustsm,dc=local
[cn=diradm] > cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local
```

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

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

Please enter the TCP ports for the Certificate Authority 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 Cryptoki Library.
> /opt/nfast/toolkits/pkcs11/libcknfast.so
Choose one of:
1. nCipher Corp. Ltd  SN : 612e2474f2bad82d SLOT : 761406613
> 1



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

Enter the algorithm that Certificate Authority 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] >

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] >

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] >

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] >

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] >

================================================================================
 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 Certificate Authority 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 Certificate Authority.
>
easm_entrust: Successfully connected to PostgreSQL.
The Entrust schema does not exist. Certificate Authority Configuration will now
apply the Entrust schema.
Applying and configuring full DB structure...
```

```
easm_entrust: Successfully applied initial DB structure.
easm_entrust: Successfully configured DB structure.

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] >

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] >
1

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


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

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

================================================================================
 Certificate Authority 10.0.31 Configuration Review
```

```
================================================================================

1. Directory Comms:         10.194.148.84+389, LDAPv3, Binary
2. CA DNs, CRLs:            ou=CAentry,dc=entrustsm,dc=local;
cn=FirstOfficer,ou=CAentry,dc=entrustsm,dc=local
3. Dir Admin:               cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local
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. Certificate Authority 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 Certificate Authority 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 Certificate Authority 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 : 612e2474f2bad82d
    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 Certificate Authority 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


Entrust CA is initialized and Certificate Authority service is running.
```

Chapter 6. Test the integration

Steps to test integration:

1. Initialize Entrust Certificate Authority
2. Launch an Entrust Certificate Authority shell
3. Show the Entrust Certificate Authority status
4. Show the Entrust nShield HSM status
5. Import a key from the Entrust Certificate Authority database
6. Export the key from the nShield HSM to the Entrust Certificate Authority database
7. List all keys
8. List all certificates
9. Back up Entrust nShield HSM Security World files

6.1. Initialize Entrust Certificate Authority

If the Certificate Authority is not initialized:

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"
```

6.2. Launch an Entrust Certificate Authority shell

1. Before doing so, change the primary group of each user:

```
% sudo usermod -g eca Master1
% sudo usermod -g eca Master2
% sudo usermod -g eca Master3
```

To launch an Entrust Certificate Authority 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:

```
[Master1@entrust-sm-linux Master1]$ entsh
Entrust Authority (TM) Certificate Authority Control Command Shell 10.0.20(183)
Copyright 1994-2020 Entrust. All rights reserved.

Type 'help' or '?' for help on commands
entsh$
```

Further commands during testing are executed inside the Certificate Authority Shell.

6.3. Show the Entrust Certificate Authority status

To show the Entrust Certificate Authority status:

1. Open a Certificate Authority Shell, see Launch an Entrust Certificate Authority shell.
2. Type the following command. It may take several minutes for all the services to be up.

```
entsh$ service start
entsh$ service status
Checking service status...
amb     Maintenance               enabled   up    1/1 processes
ash     Admin Service Handler     enabled   up    4/4 processes
backup  Automatic Backup          enabled   up    1/1 processes
cmp     PKIX-CMP                  enabled   up    2/2 processes
integ   Database Integrity Check  enabled   up    1/1 processes
keygen  Key Generator             enabled   up    1/1 processes
listen  Listener Service          enabled   up    1/1 processes
rlsvc   Revocation List Service   enabled   up    1/1 processes
sep     Entrust proto-PKIX        disabled  down  0/2 processes
xap     XML Admin Protocol        enabled   tran  1/2 processes
```

6.4. Show the Entrust nShield HSM status

To show the Entrust nShield HSM status:

1. Open a Certificate Authority Shell, see Launch an Entrust Certificate Authority shell.
2. 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 : a165a26f929841fe 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 ****

ou=CAentry,dc=entrustsm,dc=local.Master1 $
```

6.5. Import a key from the Entrust Certificate Authority database

To import a key from the Entrust Certificate Authority database to the Entrust nShield HSM:

1. Open a Certificate Authority Shell, see Launch an Entrust Certificate Authority shell.
2. Type the following command and 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 : a165a26f929841fe SLOT : 761406613
3. Cancel operation
> 2
Checking cluster status...

The cluster will be stopped and the CA key updated.
Do you wish to continue (y/n) ? [y]
Stopping cluster...

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

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

```
Starting cluster...

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=CAentry,dc=entrustsm,dc=local.Master1 $
```

6.6. Export the key from the nShield HSM to the Entrust Certificate Authority database

To export the key from the nShield HSM to the Entrust Certificate Authority database:

1. Open a Certificate Authority Shell, see Launch an Entrust Certificate Authority shell.
2. Type the following command and select **Software** 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 : a165a26f929841fe SLOT : 761406613
3. Cancel operation
> 1
Checking cluster status...

The cluster will be stopped and the CA key updated.
Do you wish to continue (y/n) ? [y]
Stopping cluster...

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

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

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] 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=CAentry,dc=entrustsm,dc=local.Master1 $
```

6.7. List all keys

To list all keys:

1. Open a Certificate Authority Shell, see Launch an Entrust Certificate Authority shell.
2. Type the following command. Notice keys in both the Certificate Authority 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=CAentry,dc=entrustsm,dc=local
serial number:                00EA078000BF7000CA7AE74BF04D102506
current CA certificate:       N
CA certificate issue date:    Tue Feb 28 16:38:35 2023
CA certificate expire date:   Mon Feb 28 17:08:35 2033
subject key identifier:       0AF8F1EF5267734EDCCD8E236E9C3DE50B97E2FA
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:              GBx0/RIFlFXEnTMXJZITs9Ye9KQ=
hardware status: Loaded >> 'nCipher Corp. Ltd  SN : a165a26f929841fe SLOT : 761406613'.

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

Internal key index:           2
CA certificate issued by:     ou=CAentry,dc=entrustsm,dc=local
serial number:                00CC12A24A27C91E4D276DC9FBE38BE9D9
current CA certificate:       N
CA certificate issue date:    Tue Feb 28 18:38:48 2023
CA certificate expire date:   Mon Feb 28 19:08:48 2033
subject key identifier:       999087C0197A1F2B78E23A9E2C300D122FE939E1
```

```
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:              oiwieKDsyacnT1vf1F/7Pq91LfE=
hardware status: Loaded >> 'nCipher Corp. Ltd  SN : a165a26f929841fe SLOT : 761406613'.

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

Internal key index:           5
CA certificate issued by:     ou=CAentry,dc=entrustsm,dc=local
serial number:                0081F74C05EB674261F4A65791E56AC3AC
current CA certificate:       Y
CA certificate issue date:    Tue Feb 28 18:42:38 2023
CA certificate expire date:   Mon Feb 28 19:12:38 2033
subject key identifier:       40B6D71C76ED8B5A980EEE3F04A012907964E7A0
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:    C SW
migrated:                     N
hardware load error:          N
hardware CKA_ID:              N/A
hardware status: CA Hardware not used.

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

6.8. List all certificates

To list all certificates:

1. Open a Certificate Authority Shell, see Launch an Entrust Certificate Authority shell.
2. 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      2023/02/28 16:38:35  2033/02/28 17:08:35  yes
[2]    CA      2023/02/28 18:38:48  2033/02/28 19:08:48  yes
[3]    LINK    2023/02/28 16:38:35  2033/02/28 17:08:35  yes
[4]    LINK    2023/02/28 18:38:48  2033/02/28 17:08:35  yes
[5]    CA      2023/02/28 18:42:38  2033/02/28 19:12:38  yes
[6]    LINK    2023/02/28 18:38:48  2033/02/28 19:08:48  yes
[7]    LINK    2023/02/28 18:42:38  2033/02/28 19:08:48  yes

The certificate with serial number [5] is the current CA certificate.
```

```
Serial Numbers:
[1] 00EA078000BF7000CA7AE74BF04D102506
[2] 00CC12A24A27C91E4D276DC9FBE38BE9D9
[3] 00C3BDDF34F21FC3720DE6094F850B9355
[4] 00BA867D4755A8AA3615A619B9E60EA910
[5] 0081F74C05EB674261F4A65791E56AC3AC
[6] 00FAAB3B0087366C1755A30D87A97C6FD2
[7] 00AF7099D604B91E5D56070AAB4E67DD7F


ou=CAentry,dc=entrustsm,dc=local.Master1 $
```

6.9. Back up Entrust nShield HSM Security World files

To back up Entrust nShield HSM 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.

Chapter 7. Troubleshooting

- (-8973) Could not connect to the Entrust Certificate Authority service. Certificate Authority service may not be running
- ./config_authority.sh fails to detect the PKCS11 library
- Error encountered querying CA hardware
- (-77) Problem reported with crypto hardware
- Cannot initialize: Current Unix user does not have proper group membership to access Certificate Authority
- HSM logs show missing algorithms errors that are not configured by Certificate Authority during startup
- No Hardware Device Found
- (-2684) General hardware error
- Database backup failed during the Entrust Certificate Authority configuration
- Certificate Authority configuration fails
- nShield Edge Cluster Status

7.1. (-8973) Could not connect to the Entrust Certificate Authority service. Certificate Authority 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`.

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

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

Resolution:

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

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

7.3. Error encountered querying CA hardware

When you are configuring Certificate Authority, you see the following message:

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

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

Error encountered querying CA hardware.
```

Resolution:

1. Make sure you have an OCS card in the HSM. If a card is already inserted, take it out and insert it again.
2. After the card is in place, the script should be able to see the HSM.

7.4. (-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:

1. Ensure the `/opt/nfast/cnkfastrc` is as defined in Configure the Entrust Certificate Authority.

7.5. Cannot initialize: Current Unix user does not have proper group membership to access Certificate Authority

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 Certificate Authority.
(1) Operation not permitted
Press return to exit
```

Resolution:

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

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

7.6. HSM logs show missing algorithms errors that are not configured by Certificate Authority during startup

Certificate Authority 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 conformance.

Resolution:

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

7.7. No Hardware Device Found

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

Resolution:

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

7.8. (-2684) General hardware error

HSM Service is not available.

Resolution:

1. Ensure that any HSM service is running and responding.

7.9. Database backup failed during the Entrust Certificate Authority 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
```

7.10. Certificate Authority configuration fails

This procedure also applies when switching HSMs.

1. Stop the Entrust Certificate Authority service.

```
# sudo /opt/entrust/authority/bin/startstop.sh stop

# sudo ps -ef | grep entsh
...
Master1    75611       1  0 15:09 ?        00:00:36 entmon mon -sepsocket=3 -ashsocket=5 -cmpsocket=15
-xapsocket=17
...

# sudo kill 75611
```

2. Removed older configuration data.

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

3. Uninstall the PostgreSQL database.

```
# sudo /root/postgres/SM_PostgreSQL_11_7_RH8_installer/uninstall_postgres.sh
Uninstall log file is /tmp/pg_uninstall.log
Checking current PostgreSQL database version...
```

```
...
Uninstall-PostgreSQL: Completed successfully.
```

4. Reinstall the PostgreSQL database as described in Install the Entrust Authority database. After reinstalling, make sure to delete all three users, user home directories, and entrust group, before recreating them.
5. Reinstall the Entrust Certificate Authority as described in Install the Entrust Certificate Authority.
6. Configure the Entrust Certificate Authority as described in Configure the Entrust Certificate Authority.

7.11. nShield Edge Cluster Status

Ensure that the `entMgr.ini` file is as defined in nShield Edge pre-configuration.

The nShield Edge exhibits slower service startup times with respect to operations, which is to be expected. When checking the cluster status after initial set-up, you may encounter services with a "down" status or an "unknown" cluster status. To ensure proper initialization of the cluster and services, Entrust recommends allowing a few minutes for the system to complete the process. After sufficient time has passed, the services and cluster should display the correct status.

In some cases you will need to start the cluster manually. For example:

```
entsh$ cluster status
ca_wide_entry   disabled
localhost       enabled     quiescent **LOCAL**

entsh$ cluster start
Starting cluster...

entsh$ cluster status
ca_wide_entry   enabled
localhost       enabled     quiescent **LOCAL*
```

For more information regarding the cluster status, refer to *Certificate Authority 10.0 Cluster Management Guide Issue 4.0*, which is available on the Entrust TrustedCare Portal.

Chapter 8. Additional resources and related products

8.1. nShield Connect

8.2. nShield as a Service

8.3. nShield Edge

8.4. Entrust products

8.5. nShield product documentation