Entrust Identity Enterprise

nShield® HSM Integration Guide

28 Nov 2023

Contents

1. Introduction

This document describes how to integrate Entrust Identity Enterprise with the Entrust nShield hardware security module (HSM) as a Root of Trust for storage encryption, to protect the master keys and meet FIPS 140-2 Level 2 or Level 3.

Entrust Identity Enterprise has two master keys that are used to encrypt and sign sensitive information in the Entrust Identity Enterprise repository. Entrust Identity Enterprise has three master users.

Additionally, you can store credentials for the XAP, PIV and SCEP administrator accounts in the HSM instead of storing them in Entrust profiles (.EPF).

1.1. Product configurations

Entrust has successfully tested nShield HSM integration with Entrust Identity Enterprise in the following configurations:

Product	Version
Entrust Identity Enterprise Virtual Appliance	13.0

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

1.2.1. Connect XC

Security World Software	Firmware	Image	OCS	Softcard	Module
13.3.2	12.72.1 (FIPS Certified)	12.80.5	✓	✓	✓

1.2.2. nShield 5c

Security World Software	Firmware	Image	OCS	Softcard	Module
13.3.2	13.2.2 (FIPS Pending)	13.3.2	✓	✓	✓

1.3. Supported nShield HSM functionality

Feature	Support
Module-only key	Yes
OCS cards	Yes
Softcards	Yes
nSaaS	Yes
FIPS 140-2 Level 3	Yes

1.4. Requirements

Familiarize yourself with:

- Entrust Identity Enterprise documentation (https://trustedcare.entrust.com/).
- 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.

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

1.5. About the HSM and Entrust Identity Enterprise

You must decide whether you want to use an HSM before you initialize Entrust Identity Enterprise Server because the HSM can be specified only during initialization. You cannot add an HSM after initialization.

If you use an HSM, the HSM must be available at all times, or Entrust Identity Enterprise will stop working.

You cannot have some servers in a replicated system with HSMs and others without. Either all Entrust Identity Enterprise servers use HSMs, or none of them do.

Only a single HSM can be configured within Identity Enterprise.

2. Procedures

2.1. Prerequisites

Ensure the following prerequisites are implemented:

1. Install Entrust Identity Enterprise. Don't initialize the primary Entrust Identity Enterprise server node yet. This will be done after the Entrust Security World software is installed and configured. You cannot move the master keys to an HSM after you initialize Entrust Identity Enterprise. For more information, see the Entrust Identity Enterprise online documentation.
2. Install the Entrust nShield HSM using the instructions in the *Installation Guide* for the HSM.
3. Install the Entrust nShield Security World Software, and configure the Security World as described in the *User Guide* for the HSM.

2.2. Decide on a key protection type

Entrust Identity Enterprise master keys can be generated and protected with OCS, softcard, or module-only.

- OCS is a set of smartcards that are presented to the physical smartcard reader of a HSM, or remotely via an nShield TVD.
- Softcards are logical tokens with a passphrase.
- Module-only protection involves logical tokens with no passphrase.

For more information on OCS, softcard, and module-only protection, properties, and K-of-N values, see the *User Guide* for your nShield HSM.

You will need to create virtual slots (softcards) to store the administrator credentials in the HSM slots. There must be a slot available for each digital ID. For example, XAP Administrator and PIV Content Signer require two slots on the HSM. If you were to add a SCEP Administrator for Digital ID Mobile Enrollment, that will require a third slot.

2.2.1. Creating an OCS

Skip the remaining part of this section and go to configure the pkcs11 environment variables if using Module protection.

1. Ensure the `/opt/nfast/kmdata/config/cardlist` or `C:\ProgramData\nCipher\Key Management Data\config\cardlist` file contains the serial number of the card(s) to be presented, or an asterisk wildcard.
2. Open a command window as administrator.
3. Run the `createocs` command as described below. Follow your organization's security policy for the values of K/N, where K=1. After an OCS card set has been created, the cards cannot be duplicated.

   ```
   > createocs -m1 -s2 -N testocs -Q 1/1 -p
   ```

   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. Otherwise the authentication provided by the OCS 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
    5481cad7a4b86705678e262162e95ec9318d43e6 1/1 none-PL testocs
   ```

2.2.2. Creating a softcard

Skip the remaining part of this section and go to configure the pkcs11 environment variables if using Module protection.

1. Open a command window as administrator.
2. Run the ppmk command as described below.

   ```
   > ppmk --new "testsoftcard"
   ```

3. Verify the softcard was created:

   ```
   > ppmk --list
   ```

2.2.3. Configure the PKCS11 environment variables.

1. Edit or create the `cknfastrc` file located in `%NFAST_HOME%\cknfastrc` where `%NFAST_HOME%` is by default `C:\Program Files\nCipher\nfast` on Windows and `/opt/nfast/` on Linux.
   - If using OCS or Softcard protection:

```
CKNFAST_LOADSHARING=1
CKNFAST_NO_ACCELERATOR_SLOTS=1
```

- If using Module protection:

```
CKNFAST_LOADSHARING=1
CKNFAST_FAKE_ACCELERATOR_LOGIN=1
```

2. Add these lines for debug file:

```
CKNFAST_DEBUG=10
CKNFAST_DEBUGFILE=<file location>
```

2.2.4. Check Permissions

1. Test that permissions are correct. On the virtual appliance deployment the `entrust` user will need the correct permissions. On non virtual appliance deployments, there will be a non-`root` user that owns the identity enterprise installation. This user needs to be able to run `ckcheckinst` successfully. You will see output similar to the following:

```
[entrust@hostname ~]$ /opt/nfast/bin/ckcheckinst
PKCS#11 library interface version 2.40
                           flags 0
                  manufacturerID "nCipher Corp. Ltd               "
               libraryDescription "nCipher PKCS#11 13.3.2-353-52971"
          implementation version 13.03
        Loadsharing and Failover enabled

Slot  Status            Label
====  ======            =====
   0  Operator card     "testOCS                        "
   1  No token present
   2  Soft token        "testSC                         "

Select slot number to run library test or 'R'etry or to 'E'xit: 2
Using slot number 2.

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

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

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

Deleting test keys         ok

PKCS#11 library test successful.
```

2. Record the intended slot label and number. It will be used when initializing a primary Entrust Identity Enterprise Server node. In the example above, if using OCS

protection, slot 0 with label `testOCS` would be used.

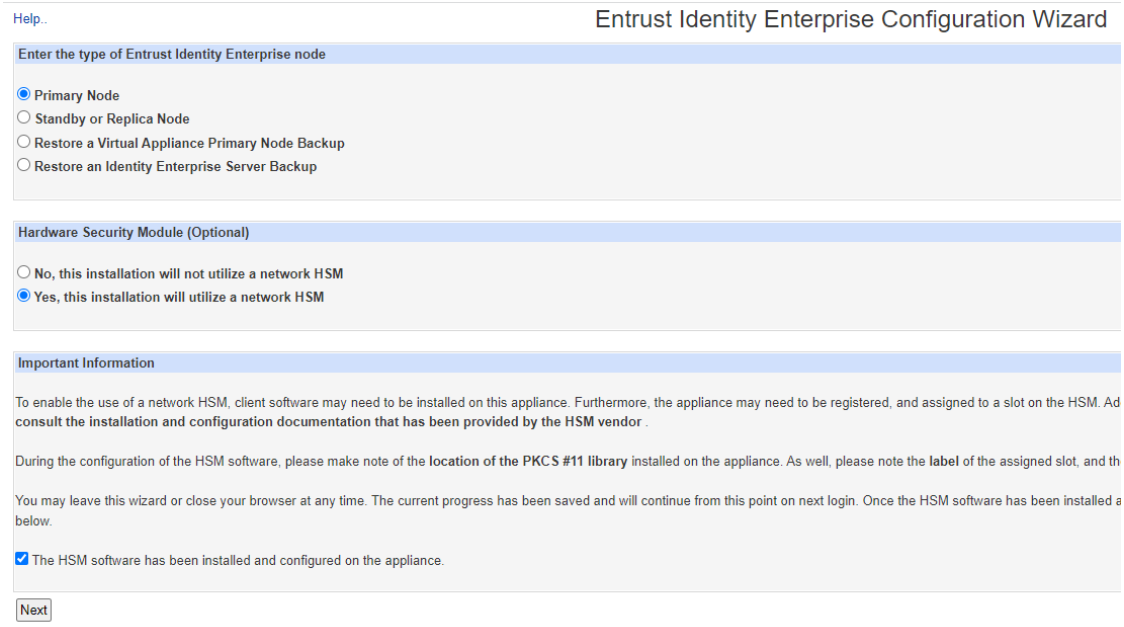
3. If `ckcheckinst` fails check the following:
    - The user is in the `nfast` group.
    - The user has read/write permissions in `/opt/nfast/kmdata/local`
    - The user has read permissions in `/opt/nfast/cknfastrc`
    - The user has read permissions in `/opt/nfast/kmdata/config`
    - The user has execute permissions in `/opt/nfast/bin`

2.3. Initialize the primary Entrust Identity Enterprise Server node

The steps to initialize the primary server node are different on virtual and non-virtual appliance deployments. For more details on the differences, see the Entrust Identity Enterprise online documentation.

2.3.1. Initialize on the Virtual Appliance Deployment

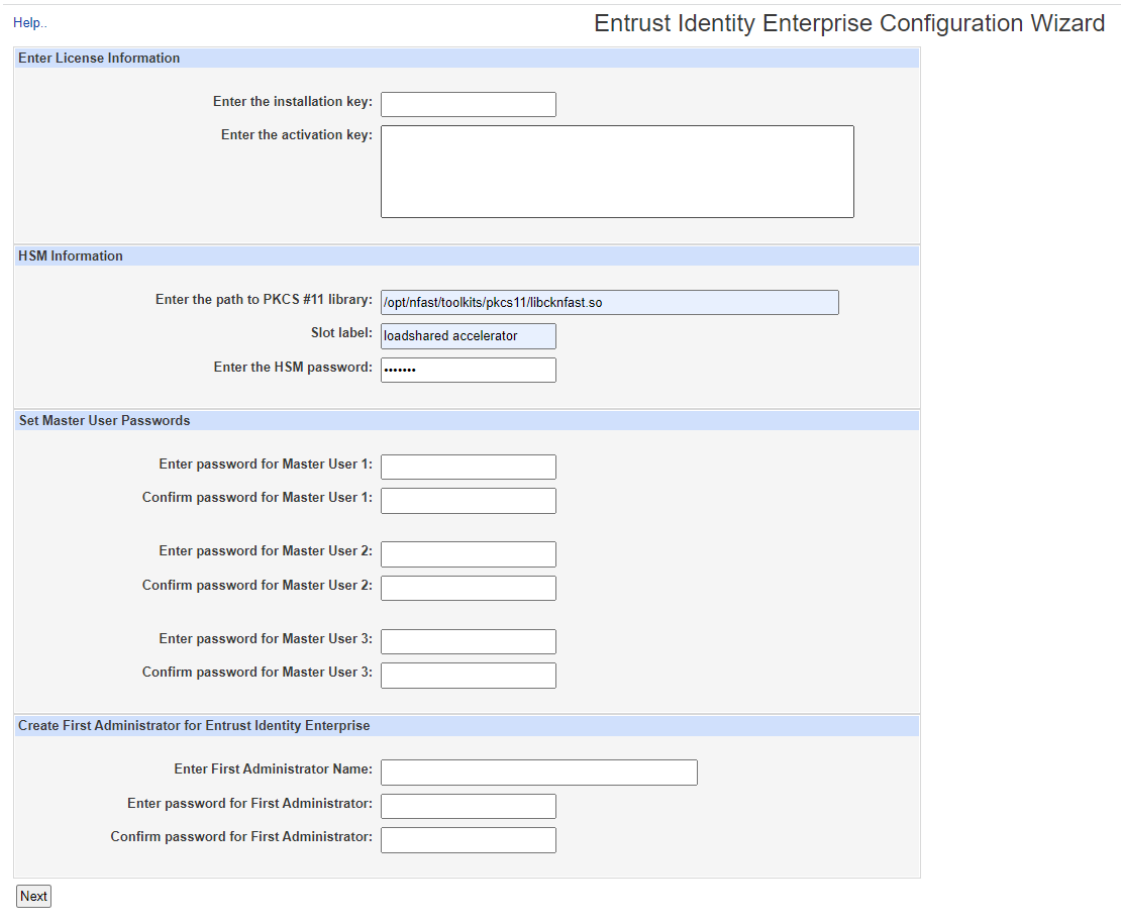
1. On the web interface, navigate through the steps of the **Entrust Identity Enterprise Configuration Wizard** until prompted to store the master keys on a hardware security module.
2. Select **Yes, this installation will utilize a network HSM**.
3. Select the checkbox next to **The HSM software has been installed and configured on the appliance**.
4. Select **Next**.



5. Enter the path to PKCS #11 library:

   ```
   /opt/nfast/toolkits/pkcs11/libcknfast.so
   ```

6. Enter the HSM **Slot label**. For module protection, this will be **loadshared accelerator**. For OCS and softcard protection, this will be the name of the cardset.
7. Enter the HSM password. For module protection, this can be any passphrase. For OCS and softcard protection, this will be the passphrase of the cardsets.



8. Complete the remaining configuration wizard.

The master keys have now been generated and stored in the HSM. All cryptographic operations using these keys are now performed within the HSM.

2.3.2. Initialize on the Non Virtual Appliance Deployment

1. Navigate through the steps of the Entrust Identity Enterprise Configuration Wizard until given the option to initialize.
2. Select the option **Do not initialize the Entrust Identity Enterprise System now.** You cannot initialize Entrust Identity Enterprise using the wizard. You must initialize Entrust Identity Enterprise using the master user shell.
3. Open the **Master User Shell**. On Microsoft Windows Server 2019 or 2016, select the

Windows button, expand Entrust Identity Enterprise in the list of applications, and select **Master User Shell**.

4. Run the **init** command as specified in the Entrust Identity Enterprise Installation document with the option **useCryptoHardware** set to **true**.
5. When prompted to provide the path to the PKCS #11 library file, enter the path to PKCS #11 library:
   - Windows

     ```
     C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll
     ```

   - Linux

     ```
     /opt/nfast/toolkits/pkcs11/libcknfast.so
     ```

6. When prompted for the HSM slot, the master user shell lists the slots and asks you to select which slot to use to store the master keys. Enter the number associated with the slot you want to use to store the master keys. This decision will depend on your key protection type choice.
7. Complete the remaining prompts of the initialization sequence.

The master keys have now been generated and stored in the HSM. All cryptographic operations using these keys are now performed within the HSM.

2.4. To create administrator accounts using the Master user shell

For more information, see the Entrust Identity Enterprise product documentation. For steps on storing XAP, PIV Content Signer and SCEP credentials in the HSM, see https://web.entrust.com/webhelp/ID-Ent_130_SmartCreds_WebHelp/.