

# Entrust PKI Hub

#### nShield<sup>®</sup> HSM Integration Guide

2025-01-17

© 2025 Entrust Corporation. All rights reserved.

### Table of Contents

1. Introduction	1
1.1. Product configuration	1
1.2. Supported nShield hardware and software versions	1
1.3. Requirements	1
2. Deploy Entrust PKI Hub	3
3. Install and configure the Entrust nShield HSM	4
3.1. Install the Entrust nShield HSM	4
3.2. Install the Entrust nShield Security World Software and create the	
Security World.	5
3.3. Edit the configuration files	6
3.4. Create the OCS	6
3.5. Create a user account	7
4. Integrate the Entrust PKI Hub and the Entrust nShield HSM	8
4.1. Make the Entrust PKI Hub server a client of the HSM	8
4.2. Configure the Entrust PKI Hub	8
5. Test the integration.	11
6. Additional resources and related products	. 12
6.1. nShield as a Service	. 12
6.2. KeyControl	12
6.3. KeyControl as a Service	12
6.4. Entrust products	. 12
6.5. nShield product documentation	. 12

## **Chapter 1. Introduction**

The Entrust PKI Hub is a versatile and robust virtual appliance that streamlines and simplifies deployment across various environments of the following Entrust solutions: Certificate Authority, CA Gateway, Certificate Enrollment Gateway, Certificate Hub, Timestamping Authority, and Validation Authority. 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 PKI Hub	v1.0

# 1.2. Supported nShield hardware and software versions

Entrust successfully tested with the following nShield hardware and software versions. All integration used OCS protection. Module-protected keys are not supported in Entrust Certificate Authority v10.0 and later versions.

Product	Firmware	Netimage
nSaaS	12.72.1 (FIPS 140-2 certified)	12.80.5
Connect XC	12.72.3 (FIPS 140-2 certified)	13.6.5
nShield 5c	13.4.5 (FIPS 140-3 certified)	13.6.5

#### 1.3. Requirements

To integrate the HSM and PKI Hub, you require:

- A dedicated virtual appliance for the installation.
- A dedicated server for hosting a PostgreSQL database and the Entrust nShield key management data.
- Access to the Entrust TrustedCare Portal.

Familiarize yourself with:

- The Entrust PKI Hub Entrust PKI Hub 1.0 Installation and Administration Guide.
- The Entrust nShield Product Documentation.
- 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.

## Chapter 2. Deploy Entrust PKI Hub

For the purpose of this integration, the Entrust PKI Hub was deployed from iso in a virtual environment. A single node was deployed. The required PostgreSQL database was deployed in a virtual Ubuntu environment.

The complete instruction set is available in the Entrust PKI Hub Entrust PKI Hub 1.0 - Installation and Administration Guide.

# Chapter 3. Install and configure the Entrust nShield HSM

This section applies to on-premises applications. In nSaaS applications, the Entrust PKI Hub gets the key management data as defined by the nSaaS service.

There are two scenarios for on-premises applications:

- An Entrust nShield HSM infrastructure already exists.
- No existing Entrust nShield HSM infrastructure.

In the first scenario, the Entrust PKI Hub pulls the key management data from the remote file system (RFS). At this point in time only Linux based RFS are supported. The RFS doesn't have to be a client of an HSM. However, it must contain the key management data (world, module file, and an OCS) in its local directory. Copy these files from an existing client to the RFS.

When no Entrust nShield HSM infrastructure exists, deploy a Linux server and install in it the security world software. Make this server a client of the HSM and create a world and OCS. After completing the configuration of the Entrust PKI Hub, this server can be removed as a client of the HSM and decommissioned.

The Entrust PKI Hub utilizes a user account to pulls the key management data from either the RFS or server. The permissions required for this account are described below.

- Install the Entrust nShield HSM
- Install the Entrust nShield Security World Software and create the Security World
- Edit the configuration files
- Create the OCS
- Create a user account

#### 3.1. Install the Entrust nShield HSM

Install the nShield Connect HSM locally, remotely, or remotely via the serial console. Condensed instructions are available in the following Entrust nShield Support articles.

• How To: Locally Set up a new or replacement nShield Connect.

- How To: Remotely Setup a new or replacement nShield Connect.
- How To: Remotely Setup a new or replacement nShield Connect XC Serial Console Model.

The complete instruction set is available at nShield v13.6.5 Hardware Install and Setup Guides.

#### 3.2. Install the Entrust nShield Security World Software and create the Security World

This section applies to the sever deployed when no Entrust nShield HSM infrastructure exists.

- 1. Install the Security World software. The complete instruction set is available at nShield Security World Software v13.6.5 Installation Guide.
- 2. Add the Security World utilities path to the system path. This path is typically /opt/nfast/bin.
- 3. Open firewall port 9004 for the Entrust nShield HSM connections.
- 4. If using remote administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).
- 5. Configure the server as a client of the Entrust nShield HSM.
- 6. Open a command window and run the following to confirm the Entrust nShield HSM is **operational**.

```
root@dev-ubuntu:~# enquiry
Server:
enquiry reply flags none
enquiry reply level Six
serial number
mode
                     operational
version
                   13.6.3
Module #1:
enquiry reply flags none
enquiry reply level Six
                    7852-268D-3BF9
serial number
                     operational
mode
                     13.2.4
version
 . . .
```

7. Create your Security World or copy an existing one. Follow your organization's security policy for this.



ACS cards cannot be duplicated after the Security World is created. You may want to create extras per your

organization security policy.

8. Confirm the Security World is **usable**.

```
root@dev-ubuntu:~# nfkminfo
World
generation 2
state 0x3737000c Initialised Usable ...
...
Module #1
generation 2
state 0x2 Usable
```

#### 3.3. Edit the configuration files

This section applies to the sever deployed when no Entrust nShield HSM infrastructure exists.

 Edit the configuration file /opt/nfast/cknfastrc, adding the lines shown below. Set the file permissions to read & execute by all.

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none
CKNFAST_LOADSHARING=1
```

- Edit the configuration file /opt/nfast/kmdata/config/cardlist. Add the serial numbers of the remote administration ready OCS smart cards, or a wild card.
- 3. Restart the Security World software.

root@dev-ubuntu:~# /opt/nfast/sbin/init.d-ncipher restart

#### 3.4. Create the OCS

OCS are smart cards that are presented to the physical smart card reader of the HSM. For more information on OCS use, properties, and k-of-N values, see Operator Card Sets (OCS).

In case of an existing Entrust nShield HSM infrastructure, you have the choice of using an existing OCS (k=1) corresponding to your world, or create a new one. The quorum k of k-of-N must be 1 for this application.

Otherwise, create an OCS card set following your organization's security policy, with k=1.



OCS cards cannot be duplicated after they are created. You may

want to create extras per your organization security policy.

#### 3.5. Create a user account

- 1. Create a user account in the RFS or server. For the purpose of this integration we named it **pkihubuser**.
- 2. Add this user to the group **nfast**.

root@dev-ubuntu:~# usermod -aG nfast pkihubuser root@dev-ubuntu:~# su - pkihubuser pkihubuser@dev-ubuntu:~\$ groups pkihubuser nfast

### Chapter 4. Integrate the Entrust PKI Hub and the Entrust nShield HSM

- Make the Entrust PKI Hub server a client of the HSM
- Configure the Entrust PKI Hub

# 4.1. Make the Entrust PKI Hub server a client of the HSM

- 1. Using the HSM front panel, add the IP of the Entrust PKI Hub server as a client of the HSM.
- 2. Present the OCS card from section Create the OCS to the HSM through the front panel card reader.

#### 4.2. Configure the Entrust PKI Hub

- 1. Login into the Entrust PKI Hub Management Console web GUI as explained in Starting up the Management Console .
- 2. In the content pane, under **Certificate Authorities**, select **Manage Solution**.
- 3. Leave the **Import configuration** and **Enable Advanced Configuration** toggle switches in the default off position. Then select **Next**.
- In the Database tab, enter the database information create in section Deploy Entrust PKI Hub. Then select Next.

For example:

ENTRUST Home Administer -	
	Certificate Authorities (CAs)
Configuration	Database
Deployment Operations	Database Connection
	0 Database URL*
	Database Name* pkihubdatabase
	Database username*
	Database password*
	Enable SSL mode for the PostgreSQL database*
	CA Certificate(s)*
	Select Files
	interop-ca-cert.pem

 In the HSM tab, enter the HSM information. In the RFS text box, enter the IP of the RFS, or server (no pre-existing Entrust nShield HSM infrastructure). Then select Next.



For the **Key unique identifier**, a name of your choice, only lowercase alphanumeric characters are allowed.

For example:

ENTRUST Home Administer -	
	Certificate Authorities (CAs)
Configuration	Database HSM
Deployment	HSM
operations	() Vendor*
	nshield
	OCS (Operator Card Set) passphrase*
	••••••
	Username to download the nShield files*
	pkihubuser
	Password to download the nShield files*
	Signing key unique identifier* 👔
	pkihubkey

 In the General tab, enter the PKI Hub hostname or IP. Then select Validate. Correct any detected configuration error until the Validate option displays no warnings.

For example:				
ENTRUST Ho	ome Administer 🔻			admin 🔻
	C	Certificate Authorities (CAs)		
Configuration	Database	HSM	General	
Deployment Operations	Hostname* 👔			
	CRL Generation (in d	ays) 👔		0
		Previous	Validate Download	Submit

7. Select Submit.

ENTRUST Home Admi		admin <del>v</del>
	Certificate Authorities (CAs)	
Configuration Deployment	Entrust On-Premises Product Deployment Status See the deployment status of Certificate Authorities (CAs) and other important information	
operations	Entrust PKI Hub is deploying your solution  1 The deployment will continue in the background if you leave this page while it is in progress.  Deployment in progress.	

8. Select **Deploy**. In the **Confirmation** pop-up window select **Yes**. After a few minutes, the configuration with the Entrust nShield HSM completes.



	Certificate Authorities (CAs)	
Configuration Deployment	Entrust On-Premises Product Deployment Status See the deployment status of Certificate Authonities (CAs) and other important information	
Operations	Deployment Information           Version: v202410180954         I Deployment Date: January 6, 2025 at 6:22 PM           Deployment Status: access         Click Deploy to update Entrust Certificate Authorities (CAs) from version v202410180954 to version v202410180954. The services will not be available during the update process.	
	Important Information           The Certificate Authority services are up and running.           To create a certificate authority (CA):           - Create a cure lote to manage the CAs.           - Create a user. Use fitnuit dentity as a Service (Dask) or Open ID Connect (ODC) users for production CAs.           Users with an internal password authemiciation build be used for testing and demonstration purposes only.           - Assign the CA role to the user.           - Login with that user and submit a request from the CAs Operations page.           Every user is a tennat and will be associated with a set of organizations. Create different users for different tenants.           CA Gateway CAI built have the form: (organization)-(caid)           CRL URE. http://         /occp/(organization)/(caid)	

### Chapter 5. Test the integration

This test consist of validating the key created in the HSM in section Configure the Entrust PKI Hub.

- 1. Login into the Entrust PKI Hub Management Console web GUI.
- 2. In the content pane, under **Certificate Authorities**, select **Manage Solution**.
- 3. Select the download arrow icon to the right of **Export Configuration**. Notice the compressed folder downloaded to your computer.



- 4. Expand the compressed folder and navigate to Downloads\pkihubconfiguration\kmdata.tar\kmdata\local. Notice the file named key\_encore\_<Key unique identifier>, where <Key unique identifier> is the value entered in Configure the Entrust PKI Hub. This file is the key blob corresponding to the key created in the Entrust nShield HSM.
- 5. For the purpose of validating the key, copy the key blob to an on-premises HSM client of the same world or server local folder /opt/nfast/kmdata/local/.
- 6. Execute the following commands. Notice the key name.

```
root@dev-ubuntu:/opt/nfast/kmdata/local# nfkminfo -k
Key list - 1 keys
AppName ncore Ident pkihubkey
root@dev-ubuntu:/opt/nfast/kmdata/local# rocs
'rocs' key recovery tool
Useful commands: 'help', 'help intro', 'quit'.
rocs> list keys
No. Name App Protected by
1 Id: pkihubkey ncore testOCS
rocs> exit
```

7. Delete this key blob from the HSM client or server. It remains in the Entrust PKI Hub.

# Chapter 6. Additional resources and related products

- 6.1. nShield as a Service
- 6.2. KeyControl
- 6.3. KeyControl as a Service
- 6.4. Entrust products
- 6.5. nShield product documentation