



ENTRUST

BeyondTrust Password Safe

nShield® HSM Integration Guide

2024-02-12

Table of Contents

1. Introduction	1
1.1. Password Safe use of HSM credentials	1
1.2. Prerequisites	1
1.3. Product configurations	2
1.4. Supported nShield hardware and software versions	2
1.5. More information	3
2. Install	4
2.1. Install the HSM	4
2.2. Install the Security World Software and creating the Security World	4
2.3. Install Password Safe on the Password Safe server	6
3. Configure an HSM with the BeyondInsight configuration tool	8
3.1. Ready for configuration	8
3.2. Add an HSM credential to BeyondInsight	8
4. Manage HSM credentials	11
4.1. Change HSM Credentials	11
4.2. Delete existing HSM credentials	11
5. Troubleshooting	12
5.1. Troubleshooting HSM Connection Error after Credential Addition	12
6. Additional resources and related products	13
6.1. Video	13
6.2. nShield Connect	13
6.3. nShield as a Service	13
6.4. Entrust digital security solutions	13
6.5. nShield product documentation	13

Chapter 1. Introduction

This document describes the integration of BeyondTrust Password Safe with an nShield Hardware Security Module (HSM).

Password Safe communicates with HSMs using a PKCS #11 API. nShield HSMs include a PKCS #11 driver with their client software installation. This allows applications to use the device without requiring specific knowledge of the make, model, or configuration of the HSM.

The Password Safe integration HSM treats the HSM as an external API that only requires credentials. Advanced configurations and features, such as high-availability implementations, are typically transparent in Password Safe. For example, the client software may allow a group of multiple HSMs to be presented as a single token in a single slot. In this case, Password Safe would access the group the same way it would access a single HSM. Configuring the group and synchronizing key data is outside the scope of the Password Safe software and must be performed according to the guidelines for the specific hardware.

1.1. Password Safe use of HSM credentials

- Password Safe only uses one set of HSM credentials to encrypt any stored credential at a given time.
- Password Safe always encrypts new or edited credentials using the latest stored set of HSM credentials.
- Password Safe supports legacy HSM credentials. Credentials that were encrypted using an older set of HSM credentials are still accessible if the HSM credential used to encrypt it has not been deleted manually.
- Archived HSM credentials remain in the Password Safe database until they are manually deleted.

1.2. Prerequisites

- The Password Safe server: A Windows Server that has Password Safe installed and the Password Safe database configured.
- A supported HSM: Configured and accessible to the Password Safe application server.

Before configuring the nShield HSM with Password Safe, the HSM client

software must be installed and configured. Follow the *Installation Guide* and *User Guide* for the HSM and use the tools in the HSM client software suite.

- The path to both the 32-bit and 64-bit PKCS #11 drivers.

These are included in the client software and are listed in *Installation Guide* for your HSM. Both driver locations are required during HSM configuration.

- The name of the token to which Password Safe should connect.

This is specified as part of the HSM configuration process.

- The PIN or password for an HSM user who can create and use keys.

This is specified as part of the HSM configuration process.

- There must be no other credentials configured in the database when the HSM configuration procedure is executed.



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

1.3. Product configurations

Entrust has successfully tested nShield HSM integration with Password Safe in the following configurations:

Product	Version
Operating System	Windows Server 2022 Standard Desktop Version
Password Safe	Password Safe 23.1
SQL Server	Microsoft SQL Server 2019

1.4. Supported nShield hardware and software versions

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

1.4.1. nShield

Product	Security World Software	Firmware	Netimage	OCS	Softcard	Module
nSaaS	13.3.2	12.72.1 (FIPS Certified)	12.80.5	✓	✓	✓
Connect XC	13.3.2	12.50.11 & 12.72.1 (FIPS Certified)	12.80.4 & 12.80.5	✓	✓	✓
nShield 5c	13.3.2	13.2.2 (FIPS Pending)	13.3.2	✓	✓	✓

1.5. More information

For more information, see the *User Guide* and *Installation Guide* for your HSM or contact Entrust nShield Support, <https://nshieldsupport.entrust.com>.



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

Chapter 2. Install

2.1. Install the HSM

Install the HSM by following the instructions in the *Installation Guide* for the HSM.

Entrust recommends that you install the HSM before configuring the Security World Software with your Password Safe Server.

2.2. Install the Security World Software and creating the Security World

To install the Security World Software and create the Security World:

1. On your Password Safe server, install the latest version of the Security World Software as described in the *Installation Guide* for the HSM.



Entrust recommends that you uninstall any existing nShield software before installing the new nShield software.

2. Create the Security World as described in the *User Guide*. Create the ACS and Softcards that you require.
3. Configure the `cknfastrc` environment variables:
 - a. Open the `C:\Program Files\nCipher\nfast\cknfastrc` file.
 - b. Add the following environment variables to the file:

```
CKNFAST_FAKE_ACCELERATOR_LOGIN=1
CKNFAST_NO_ACCELERATOR_SLOTS=0
CKNFAST_LOADSHARING=1
```

4. Update the `cardlist` file:
 - a. Go to the `C:\ProgramData\nCipher\Key Management Data\config` folder.
 - b. Open the `cardlist` file in a text editor and add an asterisk (*) to authorize all Java Cards for dynamic slots.
5. Create a Softcard that will be used with Password Safe.

When you are configuring Password Safe, you will need to use Softcard protection or module protection. If you are using a Softcard, you need to create it first.

Perform the processes in [Create a Softcard](#) on the Password Safe server, using a PowerShell terminal as **Administrator**.

2.2.1. Create the OCS

For this integration, an OCS card is required and must be inserted into the HSM to enable softcard protection for this integration.

To create the OCS:

1. Ensure file `C:\ProgramData\nCipher\Key Management Data\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.



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

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

FIPS 140-2 level 3 auth obtained.

Creating Cardset:
Module 1: 0 cards of 1 written
Module 1 slot 0: Admin Card #1
Module 1 slot 2: empty
Module 1 slot 3: empty
Module 1 slot 2: blank cardSteps:

Module 1 slot 2:- passphrase specified - writing card
Card writing complete.

cardset created; hkltu = a165a26f929841fe9ff2acdf4bb6141c1f1a2eed
```

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
a165a26f929841fe9ff2acdf4bb6141c1f1a2eed 1/1 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             2 (2)          1 of 1;
rocs> quit
```

2.2.2. 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 d9414ed688c6405aab675471d3722f8c70f5d864
```

2. Verify the Softcard was created:

```
# nfkminfo -s
SoftCard summary - 1 softcards:
Operator logical token hash          name
d9414ed688c6405aab675471d3722f8c70f5d864 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 cards
No. Name                Keys (recov) Sharing
  1 testOCS             2 (2)          1 of 1;
  2 testSC              0 (0)          (softcard)
rocs> quit
```

2.3. Install Password Safe on the Password Safe server

To install Password Safe on the Password Safe server, you have two options:

- Install BeyondInsight.

BeyondInsight includes Password Safe.

- Install a U-Series Appliance.

U-Series virtual appliances include BeyondInsight and Password Safe.

For details and installation instructions, see <https://www.beyondtrust.com/docs/beyondinsight-password-safe/index.htm>.

Chapter 3. Configure an HSM with the BeyondInsight configuration tool

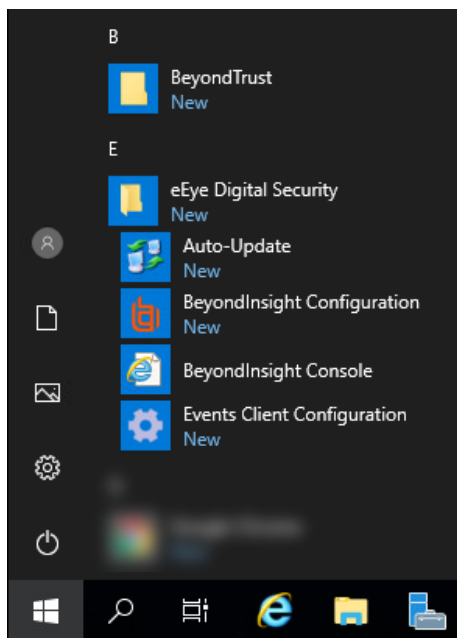
3.1. Ready for configuration

The following must be completed before configuring the HSM in BeyondInsight:

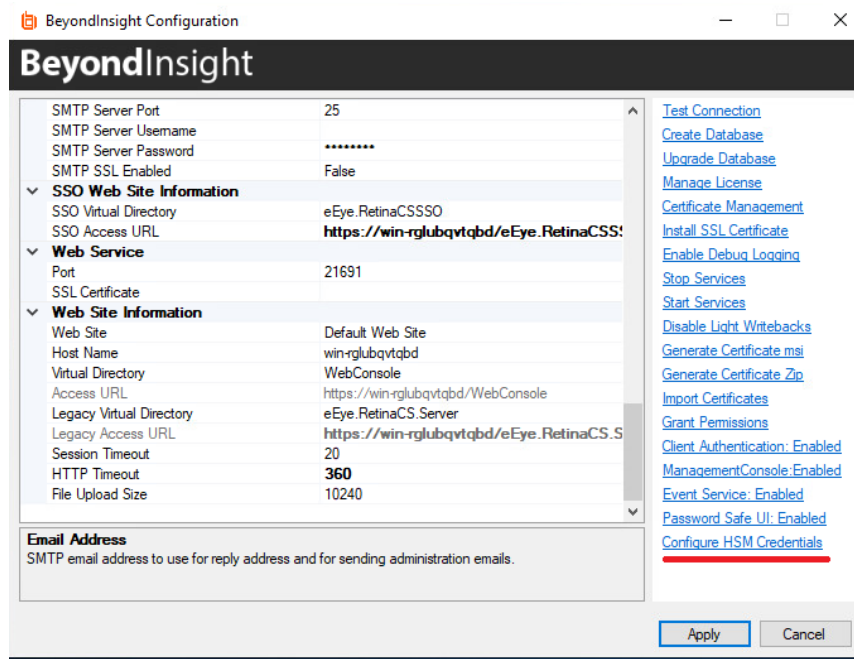
- The HSM has been installed and configured.
- The nShield client software has been installed and connected to the HSM.
- The Security World file has been created.
- A Softcard has been created using the nShield client software.
- BeyondInsight has been installed.
- Ensure the OCS card is inserted into the HSM to enable softcard protection.

3.2. Add an HSM credential to BeyondInsight

1. Sign in to the BeyondInsight server that is configured to access the HSM.
2. Open the BeyondInsight Configuration tool: **Start > Apps > eEye Digital Security > BeyondInsight Configuration**.



3. Select **Configure HSM Credentials**.



The **Configure HSM credentials** dialog appears.

4. Select **Edit > Add New HSM Credential**.

- If using softcard protection, ensure the OCS card is inserted into the HSM.

5. Enter HSM details as defined below:



The nShield HSM PKCS #11 drivers are in the **C:\Program Files\nCipher\ncfast\toolkits\pkcs1** directory.

32-bit Driver Path

Select the 32-bit PKCS #11 driver.

64-bit Driver Path

Select the 64-bit PKCS #11 driver.

Label/Slot

After a valid 32-bit/64-bit drivers have been selected, this is the list of tokens presented by the driver in the format of **label (slot number)**.

The label is the name of the HSM token. Some HSMs have a default name. Otherwise, it is the name that was set when you configured your HSM.

The slot number is an index number starting at 0. It indicates the token's position within the list of tokens presented by the driver.

Key Name

HSM keys are identified labels. A unique name must be provided for each

key. This is required to associate encrypted credentials with the key that is used to encrypt and decrypt them. Any key name can be used as long as it is unique.

Description

Information about the key, for display purposes only.

PIN

The password for the HSM token that was set up for use by BeyondInsight.

6. After inputting the HSM credentials, select **Save and Close**.
7. Reopen **Configure HSM Credentials**.
8. Initiate a connection test by selecting **Test Active Credential**. A successful test will display a dialog confirming a successful connection.
9. Close the **Configure HSM Credentials** window and **Apply** the changes in the **BeyondInsight Configuration** window.

Chapter 4. Manage HSM credentials

4.1. Change HSM Credentials



Editing an existing HSM credential might prevent Password Safe from decrypting a credential. This occurs if the encryption key name configured in the HSM credential does not match the encryption key name that was used to encrypt a credential. For this reason, editing the key name is not permitted.

To edit HSM credentials:

1. Right-click an existing credential.
2. Select **Edit Credential**.
3. Select the required cells and modify the values of:
 - 32-bit Driver Path
 - 64-bit Driver Path
 - Slot
 - Description
 - PIN
4. Select **Save**.

4.2. Delete existing HSM credentials



Deleted credentials cannot be recovered. Password Safe will be unable to decrypt any credentials encrypted with this HSM credential.

1. Right-click a credential.
2. Select **Delete Credential**.

A confirmation dialog appears.
3. Confirm the deletion.
4. Select **Save and Close**.

Chapter 5. Troubleshooting

5.1. Troubleshooting HSM Connection Error after Credential Addition

Users may experience an initial test failure and will see the following error message:

```
Test failed: Method C_Logout returned CKR_SESSION_HANDLE_INVALID.
```

The recommended steps to resolve this:

1. **Save and Exit the Current Page:** After observing the error, ensure all changes are saved and then exit the current configuration or settings page.
2. **Re-Access and Test:** Navigate back to the HSM configuration page, and then select the 'Test Active Credential' option. Often, users will receive a confirmation message:

```
HSM connection successful.
```

To further validate the successful generation and addition of the key, execute the `nkfminfo -k` command. If correctly executed, this command should show the creation of a new PKCS11 key following the HSM credential addition.

Chapter 6. Additional resources and related products

6.1. Video

6.2. nShield Connect

6.3. nShield as a Service

6.4. Entrust digital security solutions

6.5. nShield product documentation