BeyondTrust

Password Safe

Entrust nShield HSM Integration

TC:4/10/2024

Table of Contents

Password Safe Entrust nShield Hardware Security Module Integration Guide

This guide describes integrating Password Safe with Entrust nShield and nShield as a Service Hardware Security Modules (HSMs).

An HSM appliance is a hardware device that safeguards and manages digital cryptography keys for strong authentication and provides cryptographic processing functionality. A cloud-based HSM service provides cost-effective, on-demand key management services using a graphical user interface. Password Safe can use HSMs to manage encryption keys for stored credentials. The HSM takes over the key management, encryption, and decryption functionality for the stored credentials.

Password Safe communicates with HSMs using a commonly supported API called *PKCS#11*. 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 with an 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 might allow a group of multiple HSMs to be presented as a single token in a single slot. In this case, Password Safe accesses the group the same way it accesses 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. If necessary, seek assistance from the HSM vendor.

Password Safe HSM Credential Usage

- Password Safe uses only 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 them has not been deleted manually.
- Archived HSM credentials remain in the Password Safe database until they are manually deleted.

Supported Product Configurations

Operating System / Software / Hardware	Version
Database	Microsoft SQL Server 2019
Password Safe	21.3 and later releases
Entrust HSM	nShield HSM or nShield as a Service
Connect XC Firmware / Image	12.50.11 / 12.60.2
Connect + Firmware / Image	12.50.8 / 12.60.10
Security World Software	12.70.4

***Note:** Both Softcards and Module Only Keys are supported.*

Install and Configure Entrust nShield HSM

Install the HSM

The HSM must be installed and configured using the tools provided as part of the HSM client software suite. Install the nShield HSM before configuring the Security World Software with your BeyondInsight server, following the instructions in the *Installation Guide* provided by Entrust. Take note of the following values, as they are used during the client configuration step:

- **<HSM IP>:** The IP address given to your nShield Connect
- **<HSM ESN>:** The serial number of your nShield Connect
- **<HSM HKNETI>:** The HKNETI of your nShield Connect
- **<RFS IP>:** The IP address of the client hosting the Remote File System (RFS)

Install Security World Software and Create Security World

> ***Note:*** *The BeyondInsight server firewall does not allow incoming connections. Therefore, remote administration and RFS facilities are not available from this server.*

> ***Note:*** *We recommend uninstalling any existing nShield software before installing the new nShield software.*

1. On your BeyondInsight server, install the latest version of the Security World Software as described in Entrust's *Installation Guide* for the HSM.
2. Create the Security World as described in Entrust's *User Guide* for the HSM.
3. Create the ACS and Softcards you require.
4. Configure the **cknfastrc** environment variables:
   - Open the **C:\Program Files (x86)\nCipher\nfast\cknfastrc** file.
   - Add the following environment variables to the file:

   ```
   CKNFAST_FAKE_ACCELERATOR_LOGIN=1
   CKNFAST_NO_ACCELERATOR_SLOPTS=0
   CKNFAST_LOADSHARING=1
   ```

5. Update the **cardlist** file:
   - Go to the **C:\ProgramData\nCipher\Key Management Data\Config** folder.
   - Open the **cardlist** file in a text editor and add an asterisk (*****) to **authorize all Java Cards for dynamic slots**.
6. When configuring BeyondInsight, you must use Softcard protection or module protection. If using a Softcard, you must create it first. Perform the following steps on the BeyondInsight server in a PowerShell terminal as **Administrator**:

- Create the Softcard:

```
cd c:\Program Files\nCipher\nfast\bin
./ppmk -n beyondtrustsoftcard
```

- Check for the Softcard:

```
./nfkminfo -s
```

For more information on the integration of nShield HSMs and nShield as a Service with Password Safe, please see the content available from the BeyondTrust nFinity HSM Partner Program page at https://www.entrust.com/partner-directory/beyondtrust-software-inc.

Configure HSM Credentials in BeyondInsight

Ensure the following has been completed prior to configuring HSM credentials 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.

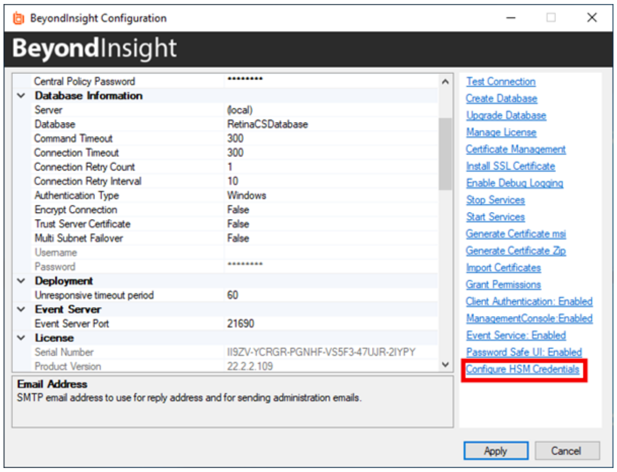
> ***Note:*** *There must not be any other credentials configured in the database when the HSM configuration procedure is executed.*

Add an HSM Credential to BeyondInsight

1. Log 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.

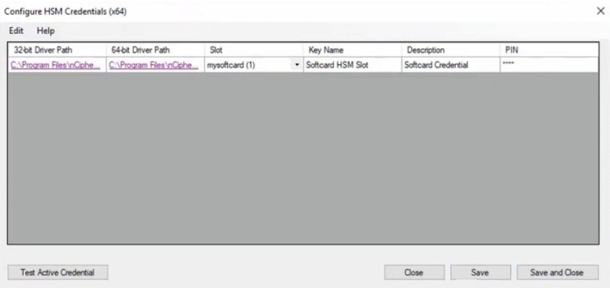
3. If a **User Account Control** dialog box appears, click **Yes** to continue.
4. Click **Configure HSM Credentials**.



Central Policy Password	*********
Database Information	
Server	(local)
Database	RetinaCSDatabase
Command Timeout	300
Connection Timeout	300
Connection Retry Count	1
Connection Retry Interval	10
Authentication Type	Windows
Encrypt Connection	False
Trust Server Certificate	False
Multi Subnet Failover	False
Username	
Password	*********
Deployment	
Unresponsive timeout period	60
Event Server	
Event Server Port	21690
License	
Serial Number	II9ZV-YCRGR-PGNHF-VS5F3-47UJR-2IYPY
Product Version	22.2.2.109

Email Address
SMTP email address to use for reply address and for sending administration emails.

5. The **Configure HSM Credentials** dialog appears. Select **Edit > Add New HSM Credential**.
6. Enter HSM details as follows:
   - **32-bit Driver Path:** Select the 32-bit PKCS #11 driver that was supplied with your HSM client software.
   - **64-bit Driver Path:** Select the 64-bit PKCS #11 driver that was supplied with your HSM client software.



32-bit Driver Path	64-bit Driver Path	Slot	Key Name	Description	PIN
C:\Program Files\nCiphe...	C:\Program Files\nCiphe...	mysoftcard (1)	Softcard HSM Slot	Softcard Credential	****

> ***Note:*** *The nShield HSM PKCS #11 drivers are located in the* ***C:\Program Files\nCipher\nFast\toolkits\pkcs1*** *folder.*

- **Slot:** After valid 32-bit/64-bit drivers are selected, this dropdown contains a list of the 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 a name set when you configured your HSM.
    - The slot number is an index number starting at **0**, which 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 to associate encrypted credentials with the key used to encrypt and decrypt them. Any key name may 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. The token must have permission to create and access keys on the HSM.

7. Click **Save**.

Manage nShield HSM Credentials

Change HSM Credentials

IMPORTANT!

Editing an existing HSM credential could prevent Password Safe from successfully decrypting the credential. This occurs if 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. In the BeyondInsight Configuration Tool, right-click an existing credential.
2. Select **Edit Credential**.
3. Click the required cells and modify the values of:
    - **32-bit Driver Path**
    - **64-bit Driver Path**
    - **Slot**
    - **Description**
    - **PIN**
4. Click **Save**.

Delete Existing HSM Credentials

IMPORTANT!

Deleted credentials cannot be recovered, and Password Safe is unable to decrypt any credentials encrypted with those HSM credentials.

To delete HSM credentials:

1. In the BeyondInsight Configuration Tool, right-click an existing credential.
2. Click **Delete Credential**.
3. Confirm the deletion.
4. Click **Save and Close**.