BeyondTrust

BeyondInsight
Thales HSM User Guide 6.9

TC:5/6/2019

Table of Contents

BeyondInsight Thales Hardware Security Module User Guide

A Hardware Security Module (HSM) is a device that safeguards and manages digital cryptography keys for strong authentication and provides cryptographic processing functionality. An HSM takes over the key management, encryption, and decryption functionality for stored credentials. This document provides the procedures to configure and manage an HSM for use within BeyondInsight.

BeyondInsight HSM Credential Usage

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

Configure a Thales HSM Using the BeyondInsight Configuration Tool

BeyondInsight communicates with HSM appliances using a commonly supported API called **PKCS#11**. Most HSM appliances include a PKCS#11 driver with their client software installation. This allows applications to leverage the device without requiring specific knowledge of the make, model, or configuration of the appliance.

HSM appliances vary in a number of ways depending on the model, and each appliance comes with its own documentation supplied by the vendor. Each HSM appliance will have its own set of steps and requirements for configuration and client software installation, such as ports used, network topology and architecture, client authentication protocol, and firewall rules, etc. Prior to configuring the HSM within BeyondInsight, these processes must be performed according to the documentation provided with the appliance, using the tools provided as part of the HSM client software suite.

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

Prerequisites

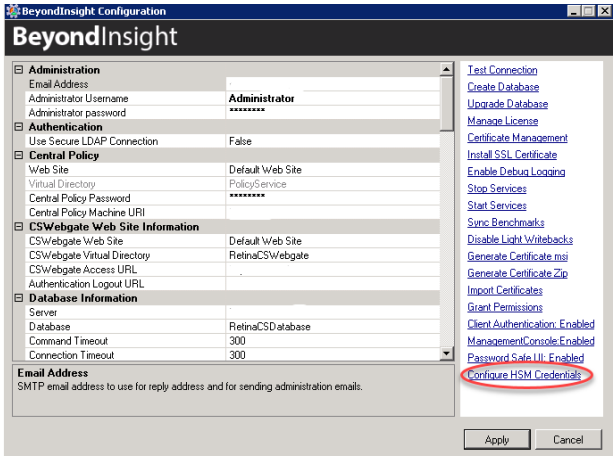
- A Windows Server with BeyondInsight installed and the BeyondInsight database configured.
- A Windows/ Linux OS with **nShield Security World Software RFS** component installed. It is not necessary for RFS to also be an nShield client, if it does not need to perform crypto.
- A supported HSM, configured and accessible to the BeyondInsight application server.
- Thales nShield HSM's require client machines to have special client software drivers installed, and may also require each client to be registered with the HSM before allowing access. This process will vary depending on the HSM device and vendor. Follow the instructions supplied by your HSM vendor to configure the BeyondInsight application server as a client.
- The path to the 32-bit PKCS#11 driver (typically included when the client software is installed and listed somewhere in the documentation provided with the appliance). The **Thales nShield Connect** driver is located by default at **%NFAST_HOME%\toolkits\pkcs11\cknfast.dll**. The driver location will be required during HSM configuration.
- The name of the token to which BeyondInsight should connect. (Specified as part of the appliance configuration process.)
- The PIN or password for an HSM user who can create and use keys. (Specified as part of the appliance configuration process.)
- There must be no other credentials configured in the database when the HSM configuration procedure is executed.

Supported Configurations

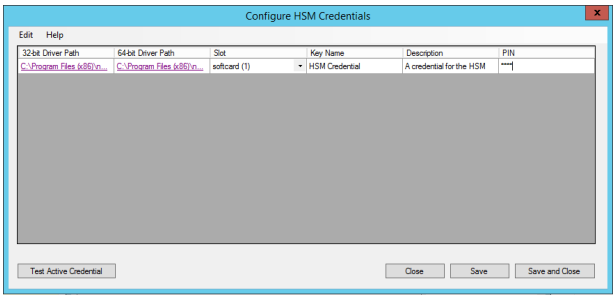
- Password Safe v. 6.2 and higher releases
- Thales nShield Connect / Security World version 12.10.01 / nShield Firmware 2.61.2
- An HSM that provides a PKCS#11 driver

Add an HSM Credential to BeyondInsight

1. Log into 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**.



5. Select **Edit > Add New HSM Credential**.
6. Enter HSM details as defined below then click **Save**.



- **32-bit Driver Path:** Select the 32-bit PKCS#11 driver that was supplied with your HSM client software. The location of the PKCS#11 driver should be provided in the documentation that came with your HSM.
- **64-bit Driver Path:** Select the 64-bit PKCS#11 driver that was supplied with your HSM client software. The location of the PKCS#11 driver should be provided in the documentation that came with your HSM.
- **Label/Slot:** After a valid 32-bit driver has been selected, this dropdown will contain 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 appliances may have a default name, otherwise it will be a name that was set when you configured your HSM. The slot number is an index number starting at 0 that 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 in order 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 PIN for the HSM user that was set up for use by BeyondInsight. The user must have permission to create and access keys on the HSM.

Set Up Thales nShield

Prior to Installation

Refer to the Thales set up guide for instructions on configuring your HSM device, setting up a new security world, and registering the BeyondInsight application as a client of the HSM. Take note of the following values, as they will be 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)

You should have received a copy of the **Thales Security World** client software installation media with your HSM. Copy the **ISO** file to the target machine.

Installation

Security World Installation:

1. Double-click to mount the **Security World ISO** on the BeyondInsight application server.
2. Run the **setup.exe** and complete the wizard using the default install options.

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

Verify Installation

Verify %NFAST_HOME% environment variable is set:

- During installation this variable should be set to **C:\Program Files (x86)\nCipher\nfast**.
- This can be verified in **Control Panel > System and Security > System > Advanced System Settings > Environment Variables**.
- The variable should be set under **System Variables** (not the user's environment variables).

Configure the Software

Add %NFAST_HOME%\bin to System PATH:

1. Edit the **System Variable PATH**, appending **;%NFAST_HOME\bin** (without quotes) to the existing value. The variable can be edited from the same location in Control Panel that was used to verify **%NFAST_HOME%** above.
2. After editing the System PATH, open **CMD** as administrator and run the `enquiry` command.
3. If the output is:
   `'enquiry' is not recognized as an internal or external command, operable program or batch file`
   either **%NFAST_HOME%** or **%PATH%** was not set properly.
4. Create a new **cknfastrc** file in the **%NFAST_HOME%** directory.
5. Add the following line in this file:
   `CKNFAST_LOADSHARING=1`

Initialize Security World

This guide assumes a Thales Security World exists. This can be created on an external RFS machine. Copy the relevant world and module files in **%NFAST_KMDATA%/local** folder on RFS into a corresponding folder on the BeyondInsight server.

BeyondTrust has successfully tested FIPS 140-2 Level 3 compliant (strictFIPS) security world with relevant FIPS authorization.

Connect to nShield

1. Open **CMD** as administrator on the BeyondInsight application server and use the commands in the following steps to configure the server as an HSM client.
2. Enroll the BeyondInsight application server as a client of the HSM:
   `nethsmenroll -f <Unit IP> <HSM ESN> <HSM HKNETI>`
3. Repeat **anonkneti** and **nethsmenroll** commands for the number of HSMs that you have configured in the pod.
4. Set up the local copy of the Remote File System:
   `rfs-setup --gang-client --write-noauth <BeyondInsight IP>`
5. Sync the RFS:
   `rfs-sync --setup --no-authenticate <RFS IP>`
   `rfs-sync --update`

> ***Note:*** *This integration has been fully tested using the softcard key protection mechanism. Support for module and Operator Card Set (OCS) key protection modes may be added in future releases.*

6. Create the softcard:
   `ppmk --new -recoverable softcard`

Backup and Restore HSM Configuration

- You must back up the **%NFAST_KMDATA%\local** directory regularly. These application token files are encrypted.
- A full restore of this directory's contents will be required for a BeyondInsight high availability configuration or while standing up a secondary BeyondInsight server for recovery purposes.
- Due to the restricted external connections, BeyondTrust recommends a manual copy of the application token files.

Manage Thales HSM Credentials

Change HSM Credentials

Editing an existing HSM credential might prevent BeyondInsight from successfully decrypting the credentials which were encrypted using the existing HSM credential.

BeyondInsight may fail to decrypt a credential 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.

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

Delete Existing HSM Credentials

IMPORTANT!

Deleting a credential is unrecoverable, and BeyondInsight will be unable to decrypt any credentials encrypted with this HSM credential.

1. Right-click a credential.
2. Click **Delete Credential**.
3. Confirm in the window that appears to continue with the deletion.
4. Click **Save and Close**.