BeyondInsight
HSM User Guide

TC:4/10/2024

Table of Contents

BeyondInsight Hardware Security Module User Guide

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.

Configure an 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 has 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. 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 that only requires credentials. Advanced configurations and features, such as high-availability implementations, are typically transparent in BeyondInsight. For example, the client software might allow a group of multiple HSM appliances to be presented as a single token in a single slot. In this case, BeyondInsight accesses the group the same way it accesses 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 BeyondInsight server, typically a U-Series Appliance. For legacy installations, this may be a Windows server that hosts BeyondInsight.
- A supported HSM, configured and accessible to the BeyondInsight instance.
- The path to both the 32-bit and 64-bit PKCS#11 drivers (typically included when the client software is installed and listed in the documentation provided with the U-Series Appliance). Both driver locations are required during HSM configuration.
- The name of the token to which BeyondInsight should connect (specified as part of the U-Series Appliance configuration process).
- The PIN or password for an HSM user who can create and use keys (specified as part of the U-Series Appliance configuration process).
- There must be no other credentials configured in the database when the HSM configuration procedure is executed.

Supported Configurations

- Password Safe v6.2 and later releases
- An HSM that provides a PKCS#11 driver

For additional information for specific HSM appliances, see:

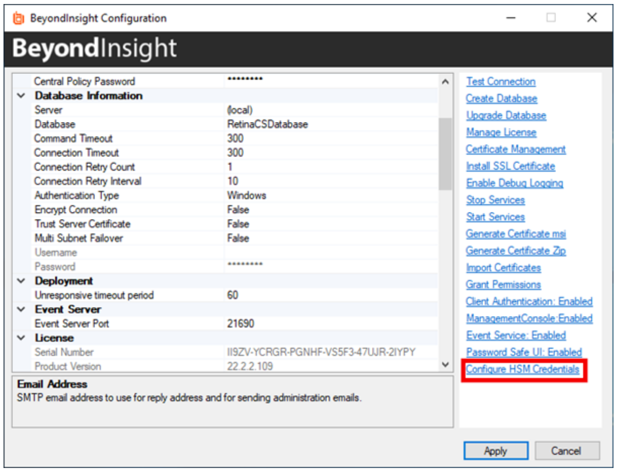
- *Dinamo Hardware Security Module Integration Guide*
- *Entrust nShield Hardware Security Module Integration Guide*
- *Thales Luna Hardware Security Module Integration Guide*

Add an HSM Credential to BeyondInsight

1. Log in to the BeyondInsight instance that is configured to access the HSM.
2. Open the BeyondInsight Configuration tool:

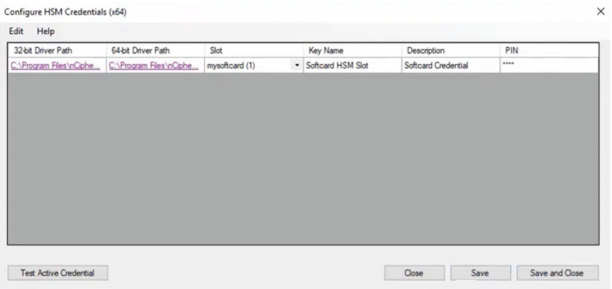
   Start > Apps > eEye Digital Security > BeyondInsight Configuration.

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, and then click **Save**.



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.



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	****

- **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 is 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 is provided in the documentation that came with your HSM.
- **Label/Slot:** After a valid 32-bit driver is 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 U-Series Appliances might 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, indicating the token's position within the list of tokens presented by the driver.

> ***Tip:** In addition to its index/position, a slot also has an ID number that might or might not match the index. Some vendors use the slot ID rather than the index when enumerating slots/tokens in their own software. For example, Gemalto's Version 5.x software uses an ID that is 1 greater than the index; meaning that what their software calls slot 1 is actually slot 0, slot 2 is actually slot 1, etc.*

- **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.

Manage 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**.