BeyondTrust

BeyondInsight

HSM User Guide 6.9

Table of Contents

BeyondInsight Hardware Security Module User Guide 3

Configure an HSM Using the BeyondInsight Configuration Tool 4

Prerequisites 4

Add an HSM Credential to BeyondInsight 4

Manage HSM Credentials 6

Change HSM Credentials 6

Delete Existing HSM Credentials 6

BeyondInsight 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 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 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 that has BeyondInsight installed and the BeyondInsight database configured.
- A supported HSM, configured and accessible to the BeyondInsight application server.
- The path to both the 32-bit and 64-bit PKCS#11 drivers (typically included when the client software is installed and listed somewhere in the documentation provided with the appliance). Both driver locations 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.

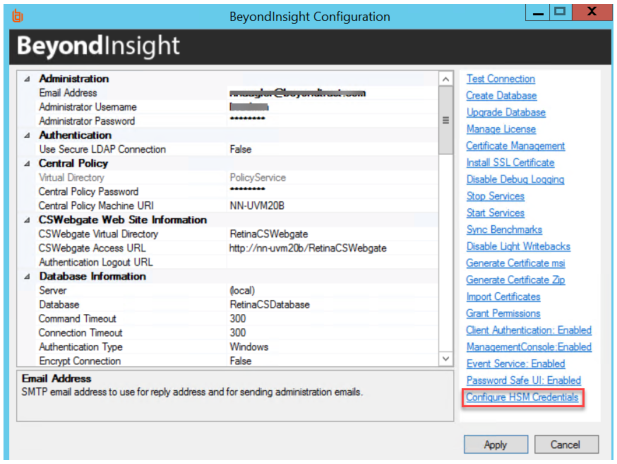
Supported Configurations

- Password Safe v. 6.2 and higher releases
- 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**.

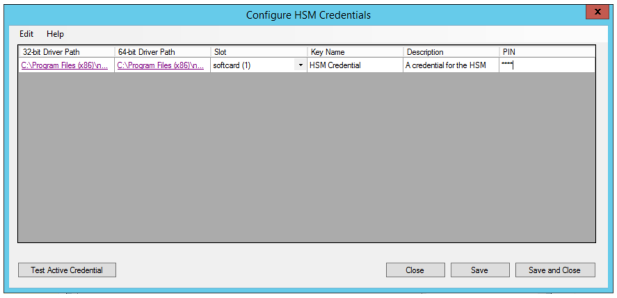


Administration	
Email Address	[redacted]
Administrator Username	[redacted]
Administrator Password	*********
Authentication	
Use Secure LDAP Connection	False
Central Policy	
Virtual Directory	PolicyService
Central Policy Password	*********
Central Policy Machine URI	NN-UVM20B
CSWebgate Web Site Information	
CSWebgate Virtual Directory	RetinaCSWebgate
CSWebgate Access URL	http://nn-uvm20b/RetinaCSWebgate
Authentication Logout URL	
Database Information	
Server	(local)
Database	RetinaCSDatabase
Command Timeout	300
Connection Timeout	300
Authentication Type	Windows
Encrypt Connection	False

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

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

6. Enter HSM details as defined below then click **Save**.



32-bit Driver Path	64-bit Driver Path	Slot	Key Name	Description	PIN
C:\Program Files (x86)\n...	C:\Program Files (x86)\n...	softcard (1)	HSM Credential	A credential for the HSM	****

- **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.

> ***Tip:*** *In addition to their index/position, slots also have an ID number that may or may not match the index. Some vendors use the slot ID instead of 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

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**.