



BeyondTrust

Password Safe Thales HSM User Guide

Table of Contents

Password Safe Thales Luna Hardware Security Module Integration Guide	3
Password Safe HSM Credential Usage	3
Supported Product Configurations	3
Configure Luna HSM Device and Luna Cloud HSM Service	4
Configure HSM Credentials in BeyondInsight	8
Manage Thales HSM Credentials	10

Password Safe Thales Luna Hardware Security Module Integration Guide

This guide describes integrating Password Safe with a Thales Luna Hardware Security Module (HSM) device and Luna Cloud HSM Service.

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
Luna HSM	Luna HSM or Luna Cloud HSM
LunaSA Firmware	7.4.x or later versions
Luna Client	10.x or later versions

Configure Luna HSM Device and Luna Cloud HSM Service

Configure Luna HSM Device

To configure the Luna HSM device, follow the below steps:



Note: For assistance, refer to the Thales product documentation for Luna Network HSM 7 and Luna HSM Client: https://thalesdocs.com/gphsm/luna/7/docs/network/Content/Home_Luna.htm

1. Ensure the HSM is set up, initialized, provisioned, and ready for deployment.
2. Create a partition to be used by Password Safe.
3. Create an exchange certificate between the Luna Network HSM and client system.
4. Register the client and assign the partition to create an NTLS connection.
5. Initialize Crypto Officer and Crypto User roles for the registered partition.
6. Ensure the partition is successfully registered and configured. The command to see the registered partitions is:

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe

lunacm.exe (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights reserved.

Available HSMs:
Slot Id ->          0
Label ->           Password Safe
Serial Number ->   1238696044904
Model ->           LunaSA 7.4.0
Firmware Version -> 7.4.0
Configuration ->   Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description -> Net Token Slot
FM HW Status ->   Non-FM
```

7. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.



Note: To configure Luna HSM High Availability (HA), refer to the Luna HSM documentation for HA. Follow the steps and details on how to configure and set up two or more HSM appliances on Windows and UNIX systems. You must enable the **HAOnly** setting in HA for failover to work so that if the primary stops functioning, all calls automatically route to the secondary until the primary starts functioning again.

Configure Luna Cloud HSM Service



Note: For assistance, refer to the Thales product documentation for Luna Cloud HSM : https://thalesdocs.com/dpod/services/luna_cloud_hsm/index.html

Standalone Cloud HSM Service Using Minimum Client Package

1. Transfer the downloaded ZIP file to your client workstation using **pscp**, **scp**, or other secure means.
2. Extract the ZIP file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system in the client install directory. Do not extract to a new subdirectory.
 - Windows: **cvclient-min.zip**
 - Linux: **cvclient-min.tar**
 - **# tar -xvf cvclient-min.tar**
4. Run the **setenv** script to create a new configuration file containing information required by the Luna Cloud HSM service.
 - Windows: Right-click **setenv.cmd** and select **Run as Administrator**.
 - Linux: Source the **setenv** script.
 - **# source ./setenv**
5. Run the **LunaCM** utility and verify the Cloud HSM service is listed.

Standalone Cloud HSM Service Using Full Client Package

1. Transfer the downloaded ZIP file to your client workstation using **pscp**, **scp**, or other secure means.
2. Extract the ZIP file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system in the client install directory. Do not extract to a new subdirectory.
 - Windows: **cvclient-min.zip**
 - Linux: **cvclient-min.tar**
 - **# tar -xvf cvclient-min.tar**
4. Run the **setenv** script to create a new configuration file containing information required by the Luna Cloud HSM service.
 - Windows: Right-click **setenv.cmd** and select **Run as Administrator**.
 - Linux: Source the **setenv** script.
 - **# source ./setenv**
5. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:
 - Cloud HSM Certificates:
 - **server-certificate.pem**
 - **partition-ca-certificate.pem**
 - **partition-certificate.pem**
 - Luna Client Certificate Directory:
 - Windows default location for Luna Client: **C:\Program Files\Safenet\Lunaclient\cert**
 - Linux default location for Luna Client: **/usr/safenet/lunaclient/cert/**



Note: Skip this step for Luna Client v10.2 or later versions.

6. Open the configuration file from the Cloud HSM service client directory and copy the **XTC** and **REST** section.
 - Windows: **crystoki.ini**
 - Linux: **crystoki.conf**
7. Edit the Luna Client configuration file and add the **XTC** and **REST** sections copied from Cloud HSM service client configuration file.
8. Change server and partition certificates path from step 5 in **XTC** and **REST** sections. Do not change any other entries provided in these sections.
 - XTC:


```
PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
```
 - REST:


```
SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
```



Note: Skip this step for Luna Client v10.2 or later versions.

9. Edit the following entry from the **Misc** section and update the correct path for the **plugins** directory:

```
[Misc]
PluginModuleDir=<LunaClient_plugins_directory>

[Windows Default]
C:\Program Files\Safenet\Lunaclient\plugins\

[Linux Default]
/usr/safenet/lunaclient/plugins/
```

10. Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.
11. Reset the **ChrystokiConfigurationPath** environment variable and point back to the location of the Luna Client configuration file.
 - Windows:
 - In **Control Panel**, search for **environment**, and select **Edit the system environment variables**.
 - Click **Environment Variables**.
 - In both list boxes for the current user and system variables, edit **ChrystokiConfigurationPath** and point to the **crystoki.ini** file in the Luna client install directory.
 - Linux:
 - Either open a new shell session, or export the environment variable for the current session pointing to the location of the **Chrystoki.conf** file:


```
# export ChrystokiConfigurationPath=/etc/
```
12. Run the **LunaCM** utility and verify the Cloud HSM service is listed.



Note: *In hybrid mode, both Luna and Cloud HSM service are listed.*

Configure HSM Credentials in BeyondInsight

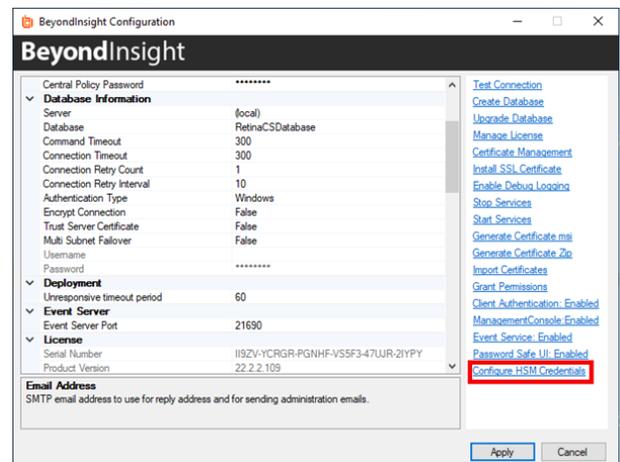
Ensure the following have been completed prior to configuring HSM credentials in BeyondInsight:

- The HSM has been installed and configured.
- The Thales client software has been installed and connected to the HSM.

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

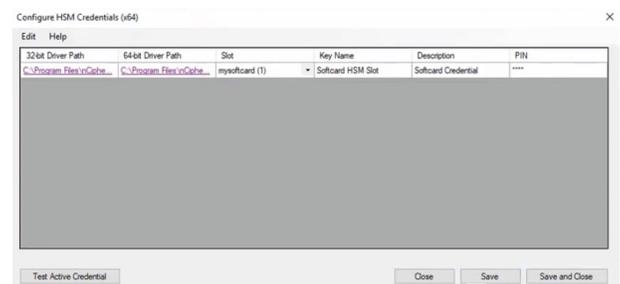
Add an HSM Credential to BeyondInsight

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**.



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.

 **Note:** The Thales HSM PKCS #11 drivers are located in the **C:\Program Files\SafeNet\LunaClient** 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 Thales 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**.