



BeyondTrust

Password Safe Dinamo HSM Integration

Table of Contents

Password Safe Dinamo Hardware Security Module Integration Guide	3
Password Safe HSM Credential Usage	3
Supported Product Configurations	3
Configure Dinamo HSM Partition	4
Configure HSM Credentials in BeyondInsight	5
Manage Dinamo HSM Credentials	8

Password Safe Dinamo Hardware Security Module Integration Guide

This guide describes integrating Password Safe with a Dinamo Hardware Security Module (HSM) device.

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

The following software and firmware versions were tested and verified as a supported configuration for this integration.

Operating System / Software / Hardware	Version
BeyondInsight and HSM Client Server OS	Windows Server 2019
Database	Microsoft SQL Server 2019
Password Safe	22.2 and later releases
Dinamo HSM	Firmware 4.0.28 and later releases
Dinamo HSM Client Software	4.7.33.0 and later releases

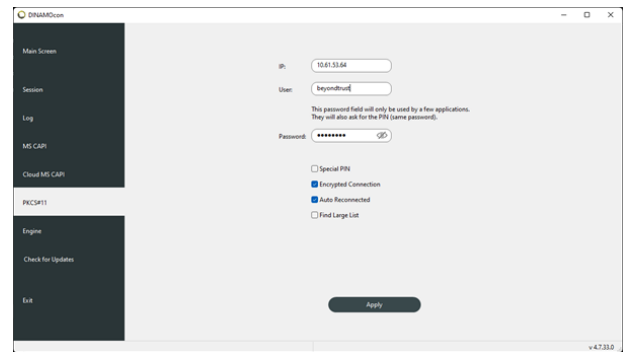
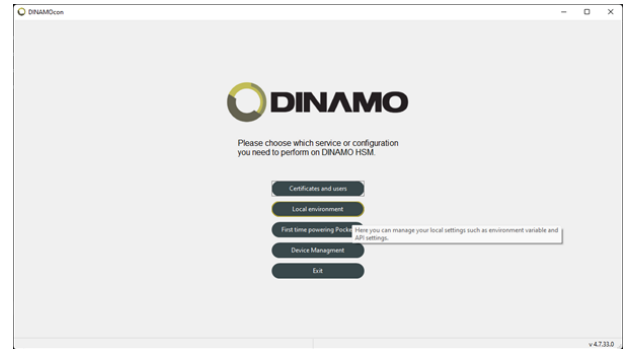


For more information on installing the Dinamo HSM Client Software on a Windows Server, please see: [HSMs Dinamo / Software Client / Windows](https://docs.hsm.dinamonetworks.io/soft_client/installation/windows) at https://docs.hsm.dinamonetworks.io/soft_client/installation/windows.

Configure Dinamo HSM Partition

Using the DINAMO Console (DINAMOcon), configure the PKCS#11 parameters with the partition credentials for use by BeyondInsight / Password Safe as follows:

1. On the home screen, click **Local environment**.
2. On the left navigation panel, click **PKCS#11**.
3. Enter the credentials of the partition to be used by BeyondInsight / Password Safe.
4. Click **Apply**.




For more information on the PKCS#11 library, please see [HSMs Dinamo / Integration / PKCS#11](https://docs.hsm.dinamonetworks.io/integration/pkcs11) at <https://docs.hsm.dinamonetworks.io/integration/pkcs11>.

Configure HSM Credentials in BeyondInsight

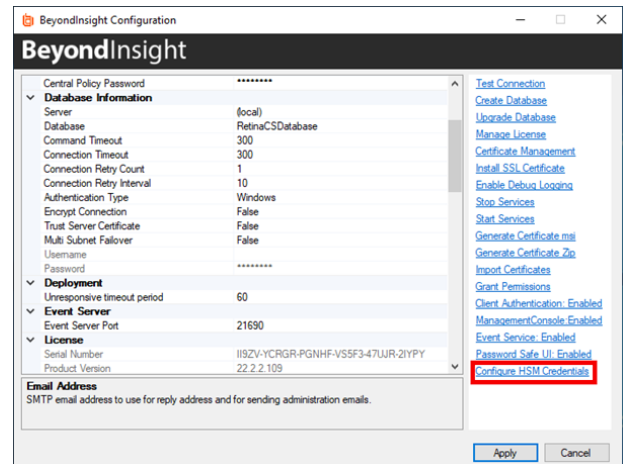
Ensure the following have been completed prior to configuring HSM credentials in BeyondInsight:

- The HSM has been installed and configured.
- The Dinamo HSM client software has been installed on the BeyondInsight server and connected to the HSM using TCP port 4433.
- The HSM partition has been configured with credentials to be used by BeyondInsight / Password Safe.
- The HSM service is started.

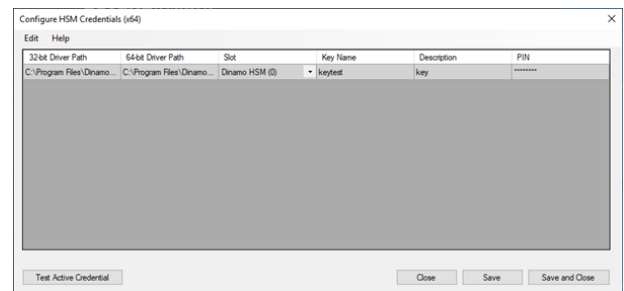
 **Note:** There must not be any other credentials configured in the database when the HSM configuration procedure is executed.

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:** Enter the 32-bit PKCS#11 driver supplied with your HSM client software. Typically located at: **C:\Program Files\Dinamo Networks\HSM Dinamo\sdk\32-bit\tacndp11.dll**.
 - **64-bit Driver Path:** Enter the 64-bit PKCS#11 driver supplied with your HSM client software. Typically located at: **C:\Program Files\Dinamo Networks\HSM Dinamo\sdk\c\tacndp11.dll**.
 - **Slot:** Select **Dinamo HSM (0)** from the dropdown.



- **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 partition credentials you configured in the Dinamo console for use by BeyondInsight / Password Safe.
- Click **Save**.
- Click **Test Active Credential**. A *HSM connection successful* message displays if the connection is successful.

Track the HSM Opening by the BeyondInsight Service

You can track the HSM session opening by the BeyondInsight service and also the symmetric key usage using the monitoring tool in the remote console (hsmcon) as shown below.

```
Dinamo - Remote Management Console v. 4.7.33.0 2018 (c) Dinamo Networks

HSM 10.61.53.64 e - Engine 5.0.28.0 (DST) - TCA0000000 - ID master

HSM - Logs - Follow

Press Control+C to exit...

2022/10/17 20:34:35 0000C42C 000B3E0D EDC1CCA3 e-conn:
10.61.53.205|10.61.53.205 10.61.53.64:4433 -
2022/10/17 20:34:35 0000C42D 000B3E10 CDEF55B7 e-conn:
10.61.53.205|10.61.53.205 10.61.53.64:4433 -
2022/10/17 20:34:35 0000C42D 000B3E11 000A3309 session thread
down [4]|10.61.53.205 10.61.53.64:4433 -
2022/10/17 20:34:42 0000C42E 000B3E12 000A3309 session thread
up [5]
2022/10/17 20:34:42 0000C42E 000B3E13 FAED60C4 10.61.53.205
auth try, c: 39, tls: y, 5|10.61.53.205 10.61.53.64:4433 -
2022/10/17 20:34:42 0000C42E 000B3E14 FAED60C4 beyondtrust
auth init, c: 39|10.61.53.205 10.61.53.64:4433 -
2022/10/17 20:34:42 0000C42E 000B3E15 FAED60C4 beyondtrust
auth ok, 10.61.53.205, 5|10.61.53.205 10.61.53.64:4433 -
^^^^^^^^^^^^^^

2022/10/17 20:34:46 0000C42E 000B3E17 FAED60C4 e-conn:
10.61.53.205|10.61.53.205 10.61.53.64:4433 -
2022/10/17 20:35:10 0000C423 000B3E2F 02C2DA21 f-sym:
beyondtrust/518bf6106ecef, 82, 0010, 0160|10.61.53.205
10.61.53.64:4433 beyondtrust

^^^^^^^^^^^^^^ ^^^^^^^^^^^^^^^

2022/10/17 20:35:10 0000C423 000B3E30 02C2DA21 f-sym:
beyondtrust/518bf6106ecef, 82, 0010, 0160|10.61.53.205
10.61.53.64:4433 beyondtrust
2022/10/17 20:35:10 0000C423 000B3E31 02C2DA21 f-sym:
beyondtrust/518bf6106ecef, 02, 0010, 0160|10.61.53.205
10.61.53.64:4433 beyondtrust
2022/10/17 20:36:49 0000C423 000B3E4B 02C2DA21 e-conn:
10.61.53.205|10.61.53.205 10.61.53.64:4433 beyondtrust
```

```
2022/10/17 20:36:49 0000C423 000B3E4C 000A3309 session thread  
down [4]|10.61.53.205 10.61.53.64:4433 beyondtrust
```

128-bit AES key generated by BeyondInsight on HSM:

```
Dinamo - Remote Management Console v. 4.7.33.125 2018 (c)  
Dinamo Networks  
  
HSM 10.61.53.64 e - Engine 5.0.28.0 (DST) - TCA0000000 - ID  
beyondtrust  
  
Keys/Objects - List  
  
Name                                     Type  
T E Label  
=====
```

518bf6106ecef n n keytest ^^^^^^^^^^^^^^	aes128
--	--------

```
Total of objects: 1  
  
Press ENTER key to continue...
```

Manage Dinamo 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**.