BeyondTrust

BeyondTrust Password Safe

24.2.1.104

Integration Guide

u.trust GP HSM Se-Series

Security Server 6.3.0

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH
	Krefelder Straße 220
	52070 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-04-10
Status	PUBLISHED
Document No.	IG-2025-0039

Table of Contents

1 Introduction

1.1 About This Guide

This guide describes the integration of Utimaco Hardware Security Modules (HSMs) with BeyondTrust Privileged Access Management (PAM) solutions to establish a secure, centralized, and compliant privileged access and key protection architecture. It provides an overview of the integration concept, prerequisites, configuration steps, and verification procedures required to securely manage privileged credentials and protect cryptographic keys using hardware-based security.

1.2 Target Audience

This guide is intended for system administrators of managing BeyondTrust Password Safe and Utimaco Hardware Security Modules (HSM).

1.3 Purpose of the Integration

The purpose of this integration is to combine BeyondTrust Privileged Access Management (PAM) with Utimaco Hardware Security Modules (HSMs) to deliver a secure, centralized, and auditable security framework for managing privileged access and protecting sensitive cryptographic material. By leveraging BeyondTrust to control, monitor, and govern privileged credentials and sessions, and Utimaco HSMs to securely generate, store, and perform cryptographic operations on encryption keys within tamper-resistant hardware boundaries, the integration reduces the risk of credential misuse, strengthens key protection, and supports compliance with regulatory and enterprise security requirements. This approach enables organizations to enforce least-privilege access, improve accountability, and establish a hardware-rooted trust model for critical security operations.

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module

Abbreviation	Meaning
PKI	Public Key Infrastructure
TDE	Transparent Data Encryption
PKCS	Public Key Cryptography Standards
PKCS#11	PKCS Part 11: The Cryptographic Token Interface Standard
SO	The PKCS#11 cryptographic slot Security Officer
DB	Database
JRE	Java Runtime Environment
MBK	Master backup key
P11CAT	the PKCS#11 graphical interface tool
CXI	Cryptographic eXtended Interface
FIPS	Federal Information Processing Standards
PAM	Privileged Access Management
GUI	Graphical User Interface
PIN	Personal Identification Number
OS	Operating System

Abbreviation	Meaning
LAN	Local Area Network
PCIe	Peripheral Component Interconnect Express
VM	Virtual Machine
DLL	Dynamic Link Library

Table 1: Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **OK**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

Table 2: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message indicates the expected result after the successful execution of an instruction.

2 Product Overview

2.1 Overview of BeyondTrust

BeyondTrust is a cybersecurity solutions provider specializing in Privileged Access Management (PAM) and identity-centric security, enabling organizations to secure, manage, and audit privileged accounts, credentials, and sessions across on-premises, cloud, and hybrid environments. Its solutions enforce least-privilege access, just-in-time elevation, and centralized credential management to reduce the identity attack surface, mitigate the risk of insider and external threats, and support compliance requirements, while providing full visibility and control over privileged activities within enterprise IT infrastructures.

2.2 Overview of GP HSM

u.trust GP HSM Se-Series is a hardware security module developed by Utimaco IS GmbH. It is a physically protected, specialized computer unit designed to perform sensitive cryptographic tasks and securely manage and store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

2.3 Joint Value Proposition

The integration of BeyondTrust Privileged Access Management with Utimaco Hardware Security Modules (HSMs) delivers a layered, defense-in-depth security model by combining centralized privileged access control with hardware-based key protection. BeyondTrust manages and monitors privileged identities, credentials, and sessions using least-privilege and just-in-time access principles, while Utimaco HSMs securely generate, store, and protect cryptographic keys within tamper-resistant hardware boundaries. Together, the solutions enhance the protection of sensitive credentials and encryption keys, reduce attack vectors associated with privileged access, and help organizations meet strict security and regulatory requirements through strong access governance, hardware-rooted trust, and comprehensive auditing.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

BeyondTrust Password Safe	Utimaco Security Server Version	Utimaco HSM
v24.2.1.104	SecurityServer 6.3.0 p11tool2 from product package Utimaco SecurityServer	SecurityServer CSe-Series/Se-Series

Table 3: Tested Versions

3.2 Hardware and Software Requirements

1. Software Requirements

Software	Software Requirements
BeyondTrust Password Safe	v24.2.1.104
HSM Utility	SecurityServer PKCS#11 Tool (p11tool2) v6.3.0
HSM Interfaces	SecurityServer PKCS#11 Provider v6.3.0
Operating System	Windows 10 or above

Table 4: Software Requirements

2. Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	u.trust GP HSM Se-Series LAN with firmware SecurityServer 6.3.0 or higher
Utimaco PCI-e HSM	u.trust GP HSM Se-Series PCI-e with firmware SecurityServer 6.3.0 or higher

Table 5: Hardware Requirements

3.3 Prerequisites

- Installed and set up SecurityServer and BeyondTrust Password Safe listed in Tested Versions.
- SecurityServer admin user.
- BeyondTrust Password Safe License.

4 Installation and Configuration

4.1 Download and Installation of Utimaco Security Server

If you have not already done so, create and request an Utimaco Support Portal Account at https://support.hsm.utimaco.com/support . This will allow you to download the software components needed for this installation.Log in to the Utimaco Support Portal, and download the u.trust GP HSM Se-Series package: https://support.hsm.utimaco.com/support/downloads/u.trust-anchor-se-series

4.2 Download and Installation of BeyondTrust Password Safe

Please refer the below link for downloading and installing BeyondTrust Password Safe. Need to complete New Appliance Deployment and New Appliance Configuration to proceed with this integration.

https://docs.beyondtrust.com/bips/docs/u-series-getting-started#deploy--import-the-virtual-machine

5 Integration Steps

5.1 Configuration on BeyondTrust Password Safe

Environment Setup.

1. Copy PKCS#11 config file `cs_pkcs11_R3.cfg` to a user-defined folder in BeyondTrust environment.
2. Copy PKCS#11 driver file `cs_pkcs11_R3.dll` to a user-defined folder in BeyondTrust environment.
3. Update the PKCS#11 config file `cs_pkcs11_R3.cfg`

```
[Global]
# For Unix:
#Logpath = /tmp
# For Windows:
 Logpath = C:/ProgramData/Utimaco/PKCS11_R3
# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 1
# Prevents expiring session after inactivity of 15 minutes
KeepAlive = true
# Set the Device to connect with
#[CryptoServer]
# Device specifier
Device = <port>@<HSM_IP>
```

4. Set the PKCS#11 R3 configuration file path using the environment variable `CS_PKCS11_R3_CFG`. In this integration, a PowerShell command is used to define and export the environment variable. Users may choose any appropriate and persistent method to configure the environment variable, provided it ensures that the variable remains available after system reboots and is not removed during user session initialization or server restarts.

```
>[System.Environment]::SetEnvironmentVariable("CS_PKCS11_R3_CFG"),"<FilePath>",
"User")
```

```
PS C:\Users\btadmin>
PS C:\Users\btadmin>
PS C:\Users\btadmin> [System.Environment]::SetEnvironmentVariable("CS_PKCS11_R3_CFG", "C:\Users\btadmin\Documents\cs_pkcs11_R3.cfg", "User")
PS C:\Users\btadmin>
PS C:\Users\btadmin>
PS C:\Users\btadmin>
PS C:\Users\btadmin>
```

Figure 1 : Setting 'CS_PKCS11_R3_CFG' environment variable

5. Verify that the environment variable is added.

```
>GetChildItem Env:
```

```
Windows PowerShell
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\btadmin> Get-ChildItem Env:

Name                           Value
----                           -----
ALLUSERSPROFILE                C:\ProgramData
APPDATA                        C:\Users\btadmin\AppData\Roaming
CommonProgramFiles             C:\Program Files\Common Files
CommonProgramFiles(x86)        C:\Program Files (x86)\Common Files
CommonProgramW6432             C:\Program Files\Common Files
COMPUTERNAME                   PSUTIMACO
ComSpec                        C:\Windows\system32\cmd.exe
CS_PKCS11_R3_CFG               C:\Users\btadmin\Documents\cs_pkcs11_R3.cfg
DriverData                     C:\Windows\System32\Drivers\DriverData
HOMEDRIVE                      C:
HOMEPATH                       \Users\btadmin
LOCALAPPDATA                   C:\Users\btadmin\AppData\Local
LOGONSERVER                    \\PSUTIMACO
MSMPI_BENCHMARKS               C:\Program Files\Microsoft MPI\Benchmarks\
MSMPI_BIN                      C:\Program Files\Microsoft MPI\Bin\
NUMBER_OF_PROCESSORS           2
OS                             Windows_NT
Path                           C:\Program Files\Microsoft MPI\Bin\;C:\Windows\system32;C:\Windows;C:\Windows\System3...
PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
PROCESSOR_ARCHITECTURE         AMD64
PROCESSOR_IDENTIFIER           Intel64 Family 6 Model 79 Stepping 1, GenuineIntel
PROCESSOR_LEVEL                6
PROCESSOR_REVISION             4f01
ProgramData                    C:\ProgramData
ProgramFiles                   C:\Program Files
ProgramFiles(x86)              C:\Program Files (x86)
ProgramW6432                   C:\Program Files
PSModulePath                   C:\Users\btadmin\Documents\WindowsPowerShell\Modules;C:\Program Files\WindowsPowerShe...
PUBLIC                         C:\Users\Public
Type here to search
```

Figure 2 : Environment Variable List

5.2 Configuration on Utimaco Security Server

5.2.1 Initialize a Slot

Initialize a slot with a custom label using the `p11tool2`.

First, create the SO or Security Officer using p11tool2. Then, using the `p11tool2` command, initialize the slot that want to use and the slot user, as shown below.

```
$ ./p11tool2 slot=<slot_no> Label=<token_label> Login=ADMIN,ADMIN.key
InitToken=<SO_PIN>
$ ./p11tool2 slot=<slot_no> LoginSO=<SO_PIN> InitPin=<CryptoUser_PIN>
```

5.3 Configuring the HSM Using the BeyondInsight Configuration Tool

1. Launch the **BeyondInsight Configuration** application: **Start** > **Apps** > **BeyondInsight Configuration**

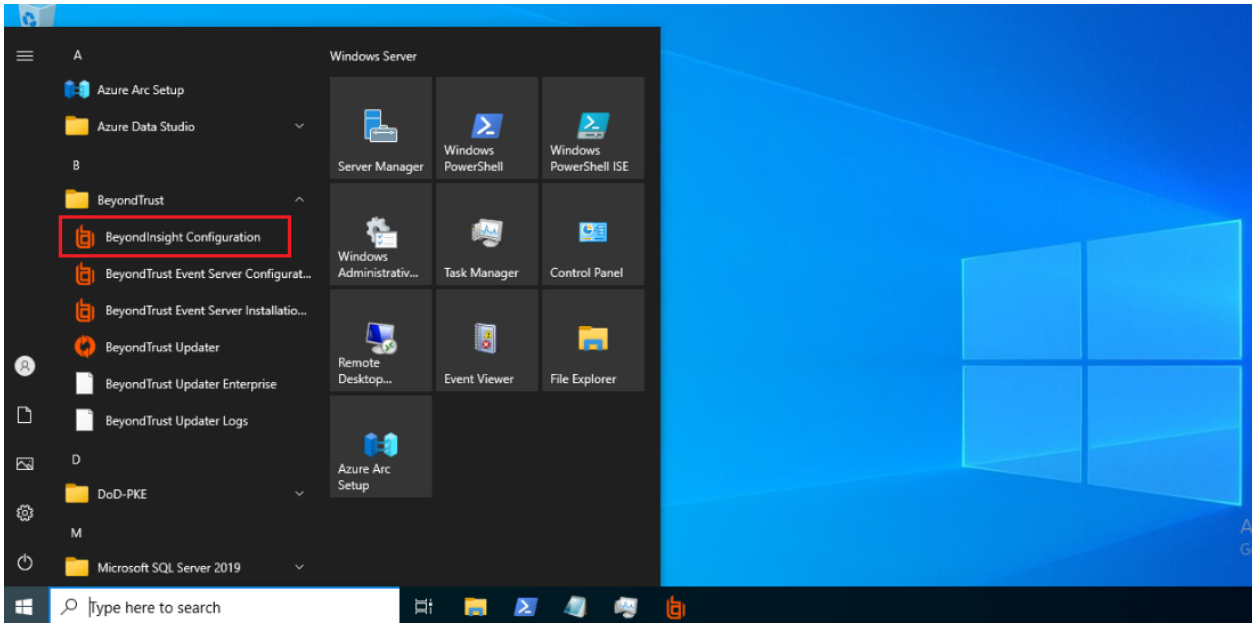

Figure 3 : Launch BeyondInsight Configuration Application

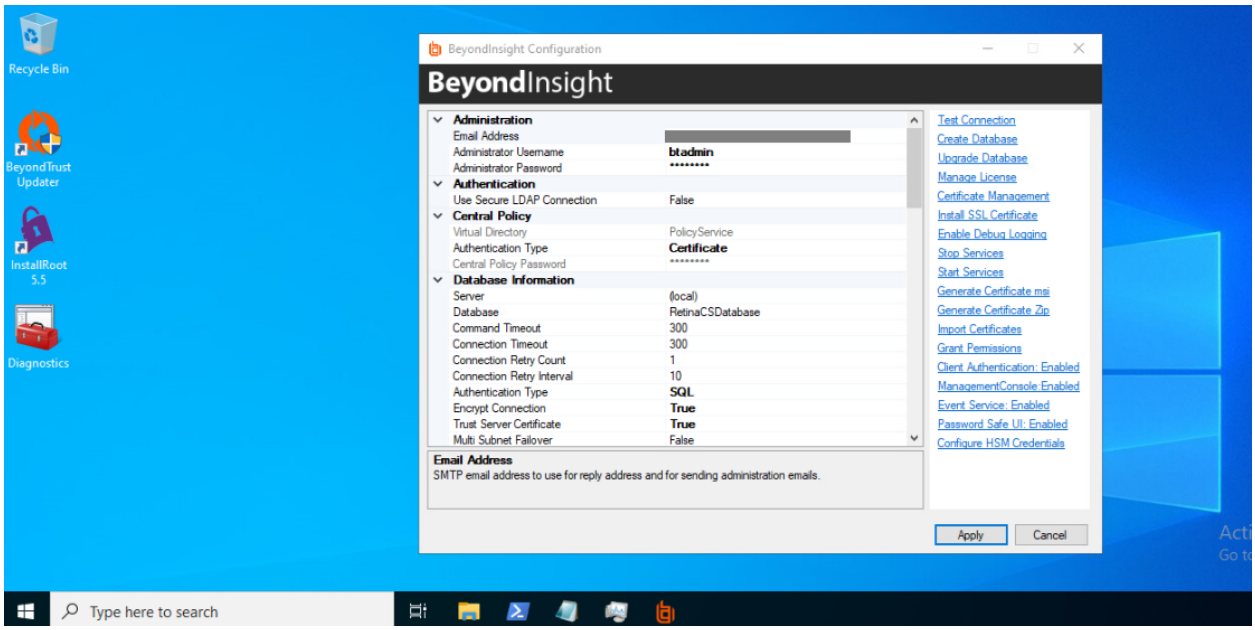

Figure 4 : BeyondInsight Application

2. Click **Configure HSM Credentials** on the right navigation pane.

   The **Configure HSM Credentials** dialog box is displayed.

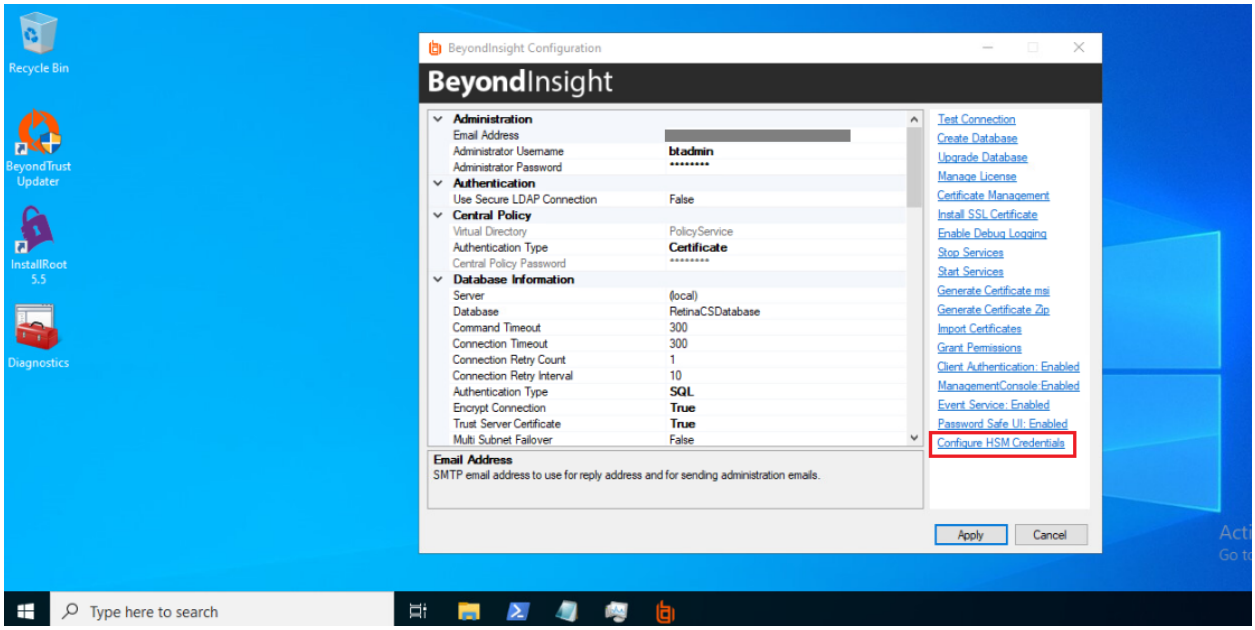

Figure 5 : Configure HSM Credentials Menu Item

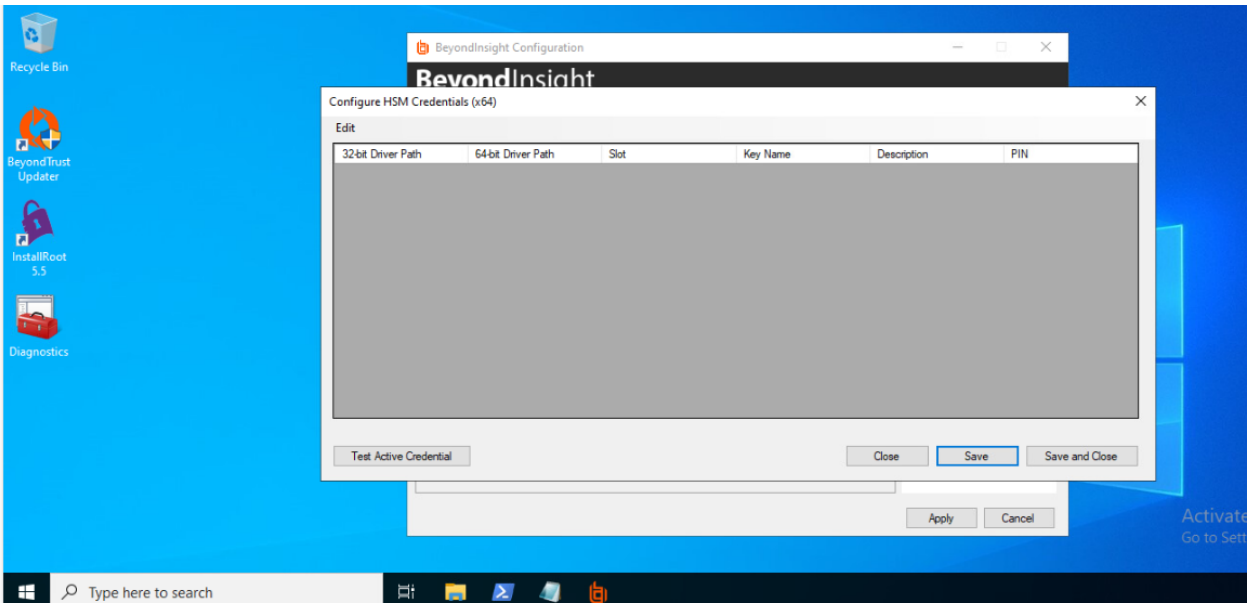

Figure 6 : Configure HSM Credentials Dialog Box

3. From the menu bar, select **Edit** → **Add New HSM Credential**.

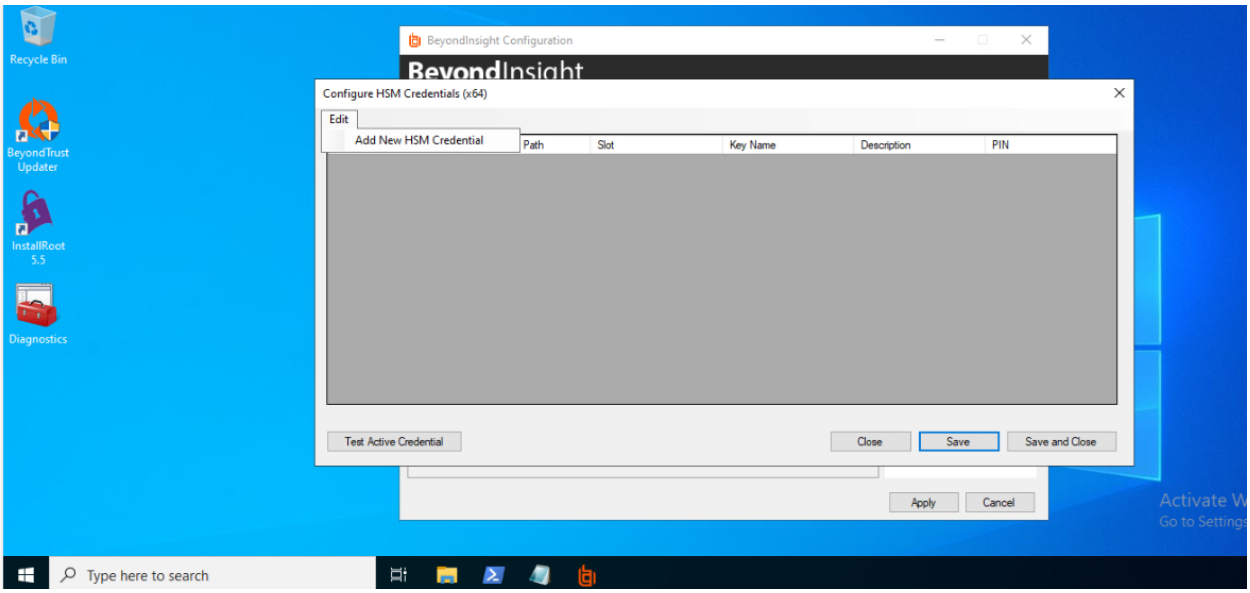

Figure 7 : Add New HSM Credential

4. In the **Add HSM Credential** dialog box, provide the following information:
   4.1. **32-bit Driver Path**: Browse to and select the 64-bit PKCS#11 provider driver.
   4.2. **64-bit Driver Path**: Browse to and select the 64-bit PKCS#11 provider driver.
   4.3. **Slot**: Select the initialized HSM slot from the drop-down list. This is the list of tokens presented by the driver.
   4.4. **Key Name**: Enter the label that uniquely identifies the HSM-protected key.
   4.5. **Description**: Enter a descriptive name or comment for the HSM key (For display purposes only).
   4.6. **PIN**: Enter the Crypto User PIN required to access the HSM token.
   4.7. Select **Save and Close** to store the HSM credential configuration.

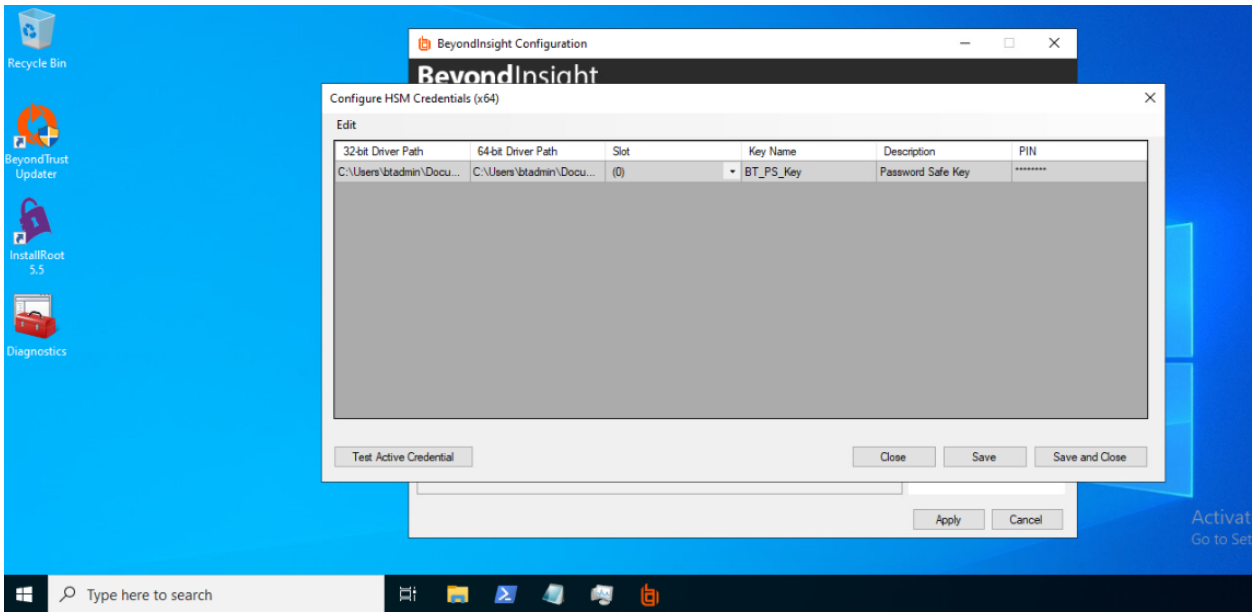

Figure 8 : HSM Credential Added

Utimaco Security Server provides only 64-bit PKCS#11 driver. Therefore, specify the same 64-bit PKCS#11 driver path in both **32-bit Driver Path** and **64-bit Driver Path** fields.

5. Reopen **Configure HSM Credentials** dialog box. Click on **Test Active Credential** button. A successful test will display a dialog confirming a successful connection with “HSM Connection Successful” message.
   A HSM key will be generated once the HSM connection is successful and generated HSM key will have the same key label as key name specified in **Key Name** field.

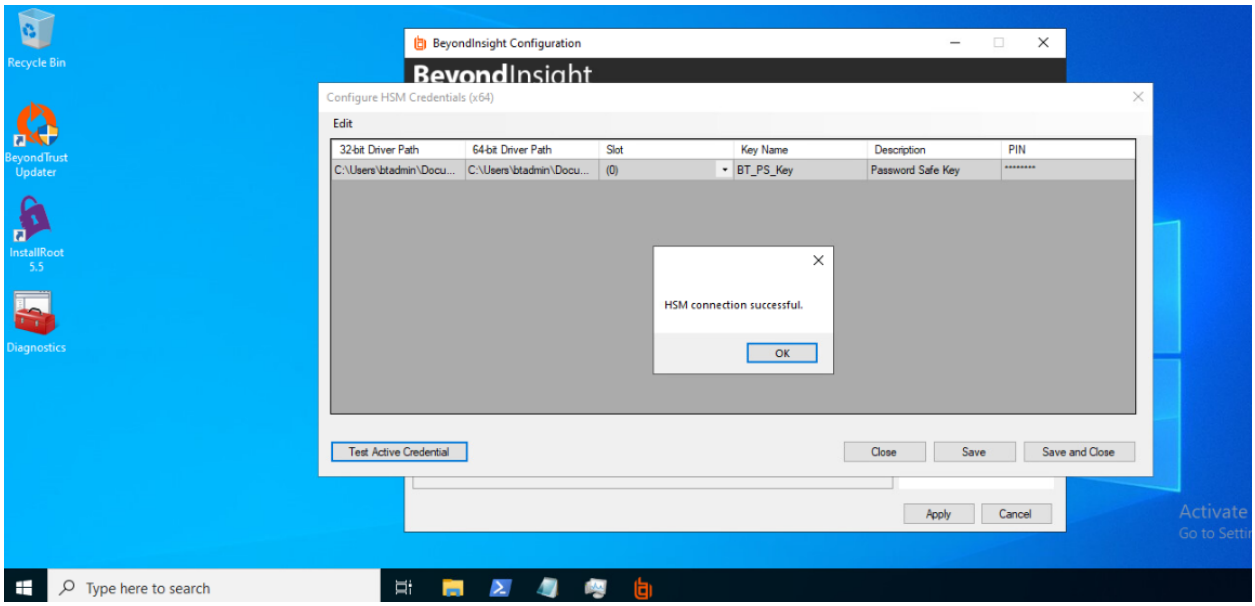

Figure 9 : HSM Connection Success

6. Close the **Add HSM Credential** dialog and Click **Apply** button in **BeyondInsight Configuration** application

7. Verify the HSM key in HSM and confirm HSM key has the same key label as key name specified in **Key Name** field.

```
[admin@master-node Administration]$
[admin@master-node Administration]$ ./p11tool2 LoginUser=87654321 ListObjects


CKO_SECRET_KEY:

+ 1.1
  CKA_KEY_TYPE                  = CKK_AES
  CKA_UNIQUE_ID                 = 16459840-EE7F-486D-835D-3CDD51A900D7
  CKA_SENSITIVE                 = CK_TRUE
  CKA_EXTRACTABLE               = CK_FALSE
  CKA_LABEL                     = BT_PS_Key
  CKA_ID                        =
                0x42545F50 535F4B65 79               |BT_PS_Key       |

[admin@master-node Administration]$
```

Figure 10 : Key Generated in HSM

6 Verification and Testing

6.1 Test Connection Check

1. Launch the **BeyondInsight Configuration** application.
2. Navigate to **Configure HSM Credentials**.
   The **Configure HSM Credentials** dialog box is displayed.
3. Click on **Test Active Credential** button. A successful test will display a dialog confirming a successful connection with “HSM Connection Successful” message.

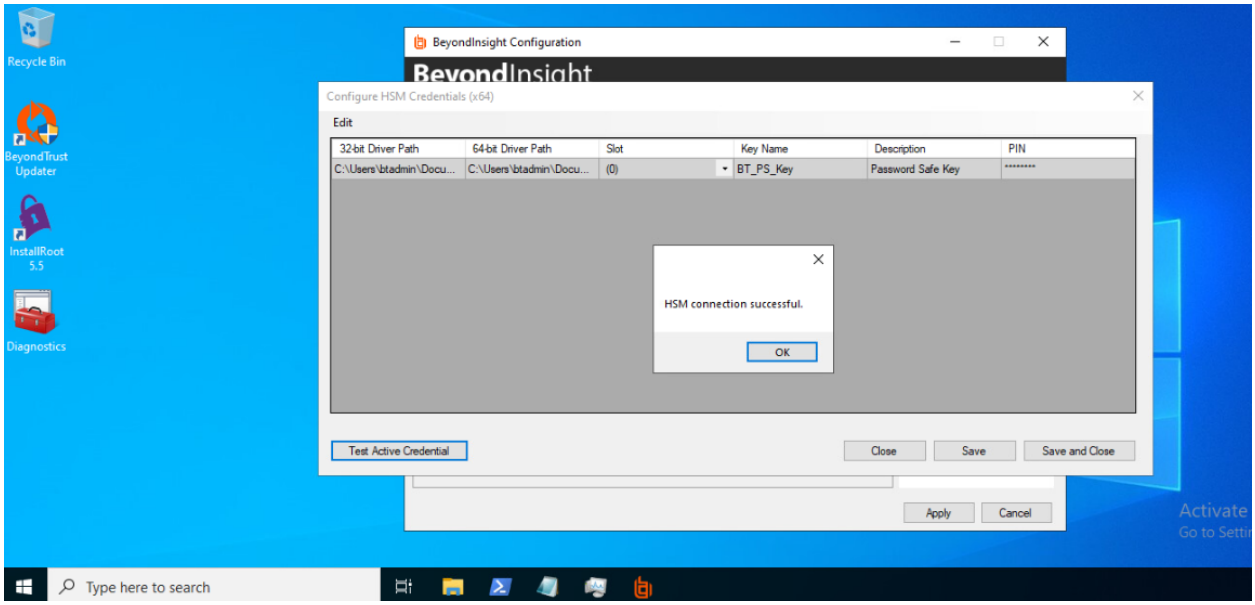

Figure 11 : HSM Connection Success

6.2 Shutdown HSM and Check Test Connection

1. Shutdown or disconnect HSM.
2. Launch the **BeyondInsight Configuration** application.
3. Navigate to **Configure HSM Credentials**.
   The **Configure HSM Credentials** dialog box is displayed.

4. Click on **Test Active Credential** button.A dialog box with the error message “Test Failed Method C_GetSessioninfo returned CKR_DEVICE_REMOVED” will be displayed

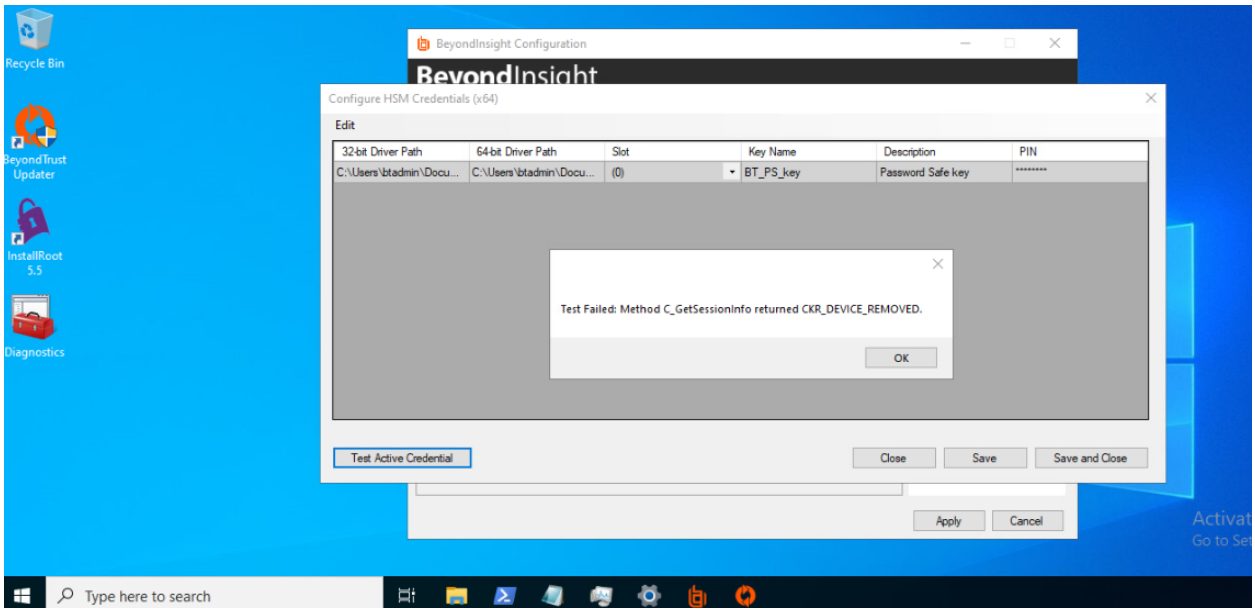

Figure 12 : HSM Connection Failed

7 Optional Features

7.1 Edit HSM Credential

To edit HSM credential;

1. Launch the **BeyondInsight Configuration** application.
2. Navigate to **Configure HSM Credentials**.
   The **Configure HSM Credentials** dialog box is displayed.
3. Right-click an existing credential.
4. Select **Edit Credential**.

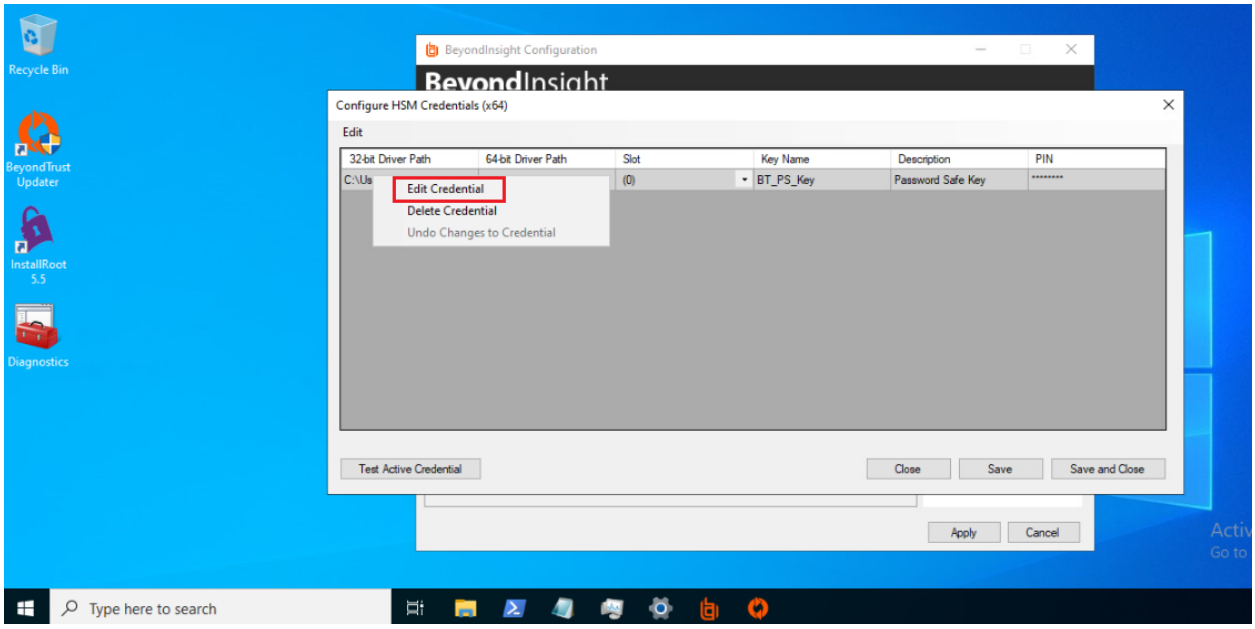

Figure 13 : Edit Credential Context Menu

5. Select the required cells and modify the values of:

- 32-bit Driver Path
- 64-bit Driver Path
- Slot (Lists only initialized slots)
- Description
- PIN

6. Select **Save**.

7.2 Delete HSM Credential

To delete HSM credential;

1. Launch the **BeyondInsight Configuration** application.
2. Navigate to **Configure HSM Credentials**.
   The **Configure HSM Credentials** dialog box is displayed.
3. Right-click an existing credential.
4. Select **Delete Credential**.

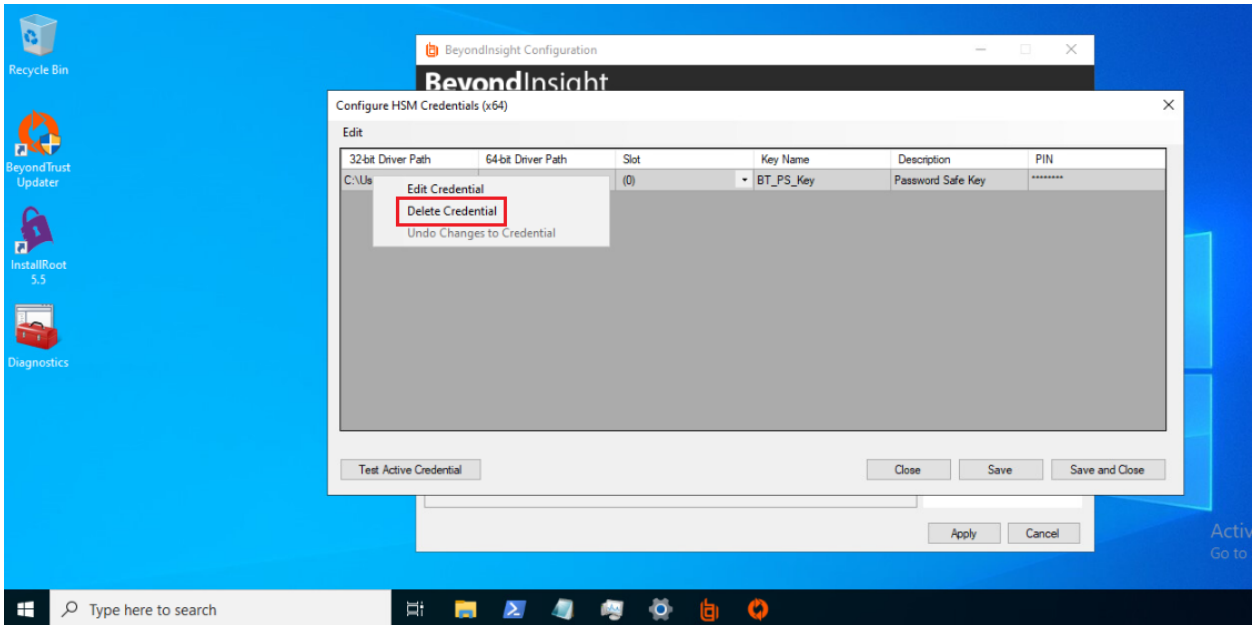

Figure 14 : Delete Credential Context Menu

5. A confirmation dialog appears with delete confirmation text. Click **Yes** button.
6. Click **Save and Close**.

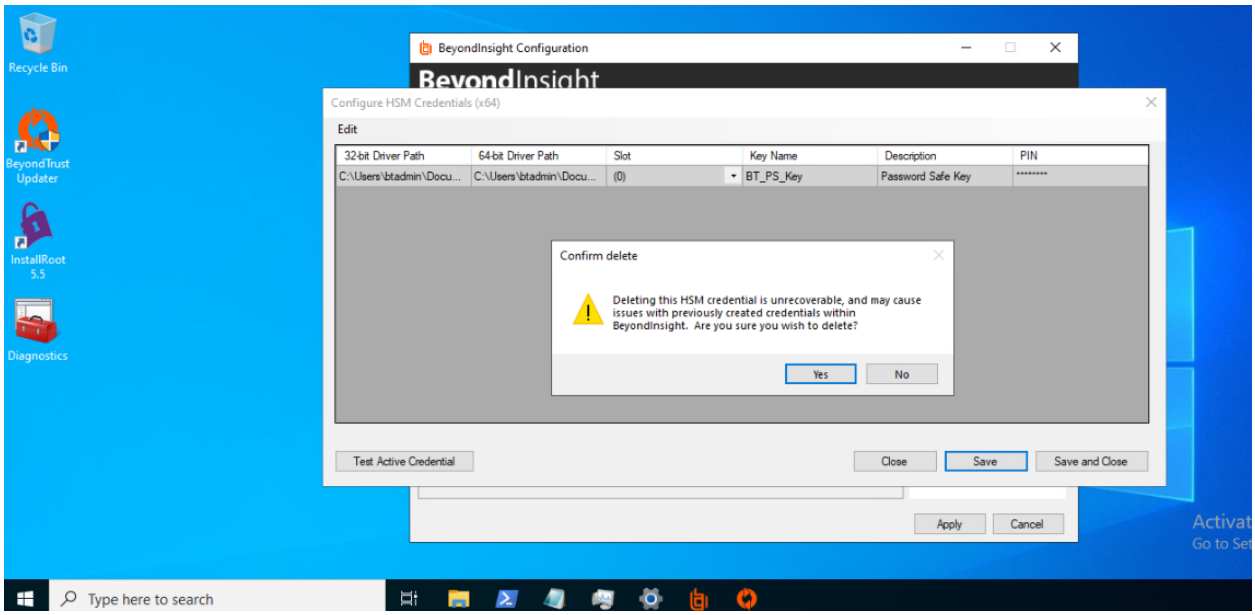

Figure 15 : HSM Credential Deletion Confirmation Dialog

Deleted credentials cannot be recovered. Password Safe will be unable to decrypt any credentials encrypted with this HSM credential

The HSM credential is removed only from BeyondTrust Password Safe. The corresponding object is not deleted from the HSM and must be removed manually by the user using the PKCS#11 `DeleteObject` command.

8 Troubleshooting

8.1 Common Issues and How to Resolve Them

Issue: Initial test failure

Description: Users may experience a test failure during the initial phase.

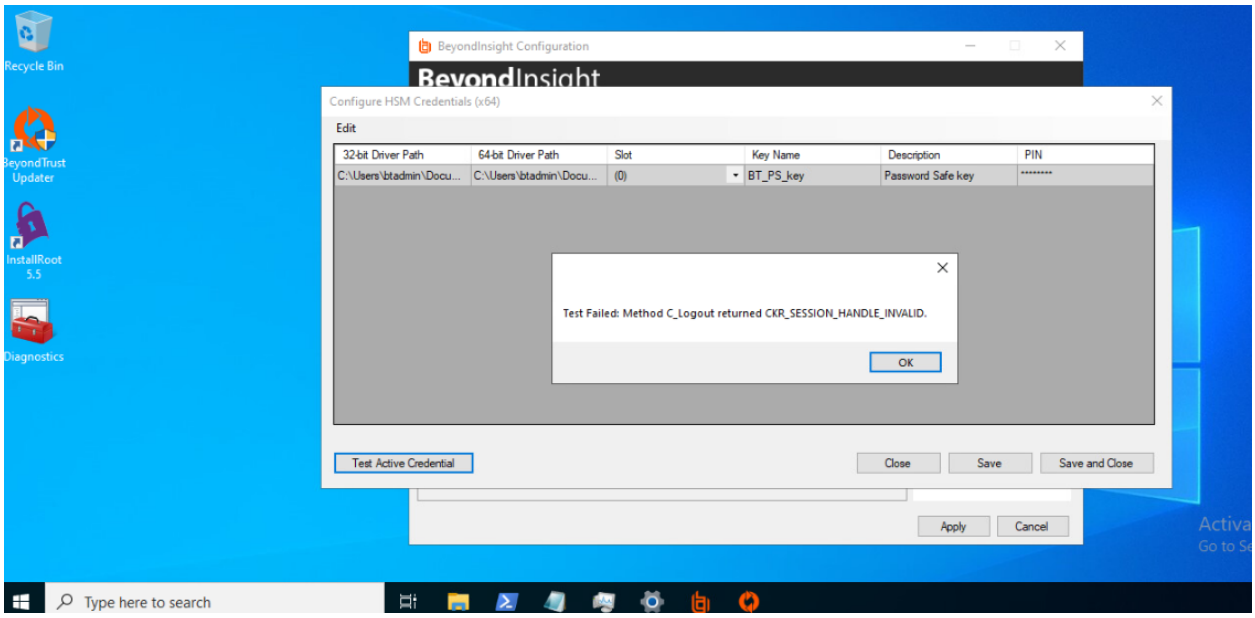

Figure 16 : Initial Test Failure

Steps to resolve:

1. Save all the changes and then exit the current page.

2. Navigate back to the **HSM configuration** page, and then click **Test Active Credential** button.

8.2 Log Locations and Interpretation

PKCS11 Log File

Log File Name: `cs_pkcs11_R3.log`

Location: Defined by the LogPath parameter in the PKCS#11 configuration file. Example: `C:/ProgramData/Utimaco/PKCS11_R3` for Windows.

Details: This log captures detailed information about PKCS#11 operations, including initialization, cryptographic actions, and error messages. The verbosity is controlled by the Logging Loglevel setting.

To simplify your testing process, it's recommended that you enable the PKCS#11 log file by adjusting the logging settings. Specifically: Set the LogPath to a writable directory (not a specific file). Set the Logging Loglevel to 1 for basic logging. Increase it to 4 for more detailed output during testing. This will generate a log file named cs_pkcs11_R3.log within the specified LogPath directory. Reviewing this log can help with troubleshooting if you encounter issues.

Once testing is complete, it's advisable to reduce Logging Loglevel to limit output to only critical or important messages

9 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Straße 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

10 Appendices

10.1 References

Title	Description	Document/Link
BeyondTrust Installation Guide	Describes the procedure for deploying and importing the BeyondTrust U-Series virtual appliance. The document covers supported hypervisors and cloud platforms, initial system configuration, and appliance setup prerequisites.	*https://docs.beyondtrust.com/bips/docs/u-series-getting-started#deploy--import-the-virtual-machine*
BeyondInsight HSM Integration Guide	Provides guidance for integrating BeyondInsight and Password Safe with external Hardware Security Modules (HSMs). The document describes supported configurations, prerequisites, and PKCS#11-based procedures for configuring and managing HSM credentials.	*https://docs.beyondtrust.com/bips/docs/bi-hsm-user-guide*

Table 6: References

10.2 Command Summary

Command	Purpose
`./p11tool2 slot=<slot_no> Label=<token_label> Login=ADMIN,ADMIN.key InitToken=<SO_PIN>`	Initialize PKCS#11 token and create Security Officer (SO) credentials

Command	Purpose
`./p11tool2 slot=<slot_no> LoginSO=<SO_PIN> InitPin=<CryptoUser_PIN>`	Initialize Crypto User PIN for the PKCS#11 slot
`[System.Environment]::SetEnvironmentVariable("CS_PKCS11_R3_CFG", "<FilePath>", "User")`	Sets the CS_PKCS11_R3_CFG environment variable at the user level to specify the Utimaco PKCS#11 R3 configuration file path used by applications to locate the PKCS#11 library configuration.
`Get-ChildItem Env:`	Displays all environment variables to verify that CS_PKCS11_R3_CFG is correctly set and available in the current user environment.

Table 7: Command Summary