Lieberman Software ERPM
Integration Guide

SafeNet
THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012997-001 (Rev A)
Release Date	April 2015

Trademarks

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimer

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Email	support@safenet-inc.com	

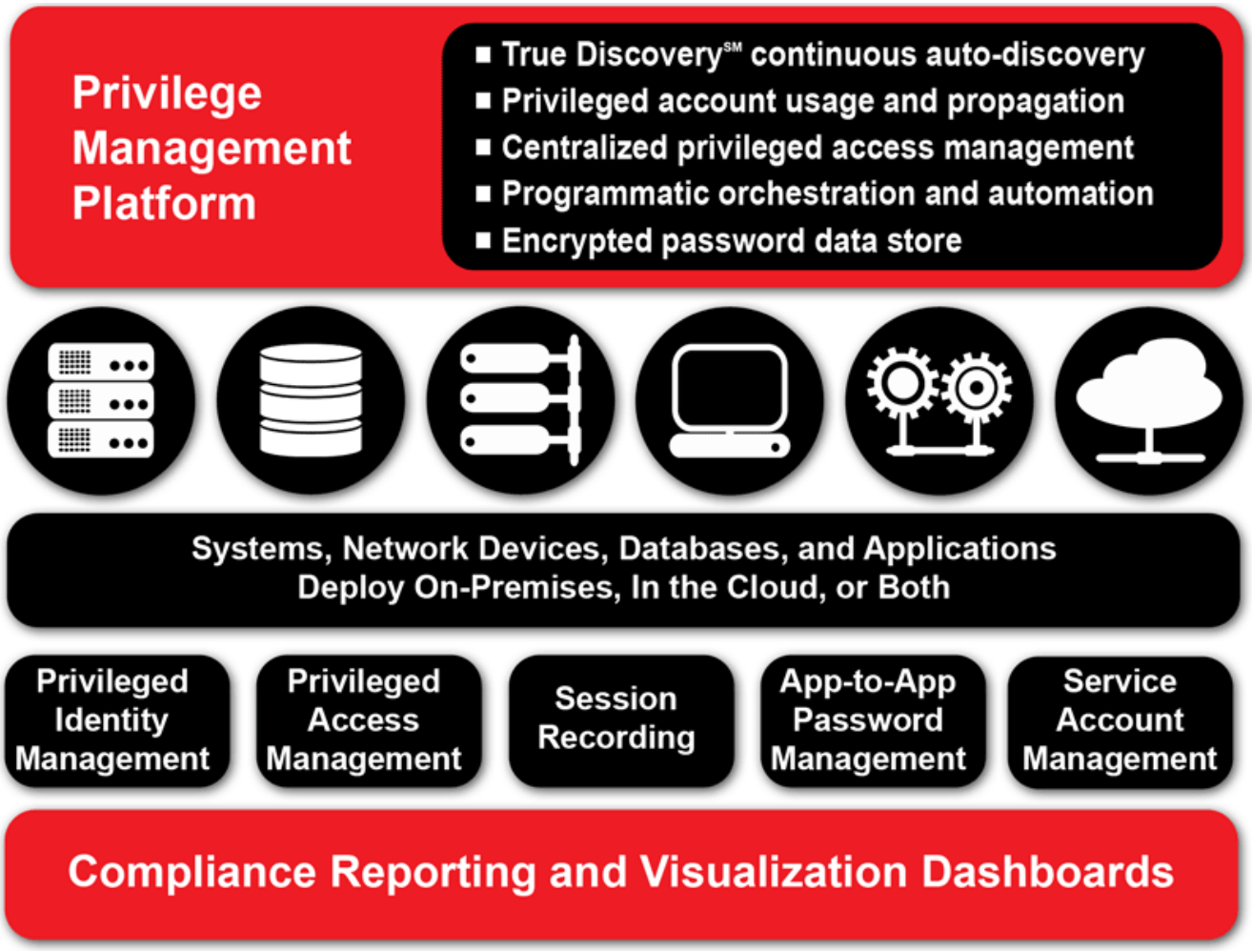
Contents

CHAPTER 1
Introduction

This document outlines the steps to configure and integrate Lieberman Software ERPM with Luna HSM.

Enterprise Random Password Manager (ERPM) is a privilege management platform that protects organizations against advanced persistent threats (APTs) and other sophisticated cyber-attacks. It ensures that powerful privileged identities are only available to audited users on a temporary, delegated basis - preventing unauthorized and anonymous access to systems with sensitive data.

This strategic privilege management solution is designed to improve the efficiency of your IT operations. It leads the market in automation to better address the complex shared account problems found in every enterprise.



ERPM secures privileged identities throughout your IT infrastructure, including:

Super-user login accounts utilized by individuals to change configuration settings run programs and perform other IT administrative duties.

Service accounts that require privileged login IDs and passwords to run.

As this privilege management product continuously tracks privileged accounts on your network, it changes each account's password to a unique and complex value. ERPM then deploys the password changes wherever they are used, and grants fast, audited access for authorized IT staff.

ERPM can help you eliminate the shared credentials that attackers exploit to gain lateral access within networks. Even if an attacker obtains a user name and password, the information is of little value because ERPM makes each privileged password unique, and frequently changes each password. Disclosed credentials are randomized immediately after use, so no one retains long-term knowledge of password secrets and every request for access is attributed to an individual.

Lieberman ERPM will use the encryption keys stored on Luna HSM. The SafeNet Luna HSM (Hardware Security Module) secures the ERPM encryption keys within an industry standard FIPS 140-2 level 3 validated HSM.

Scope

3rd Party Application Details

- Lieberman Software ERPM v4.83.8

Supported Platforms

- Windows Server 2012 R2

HSMs and Firmware Version

Lieberman ERPM has been tested with the following:

- Luna SA f/w 6.21.0 with Luna Client s/w v5.4.1 (32 bit)

Prerequisites

Luna SA Setup

Please refer to the Luna SA documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started ensure the following:

- Luna SA appliance and a secure admin password.
- Luna SA, and a hostname, suitable for your network.
- Luna SA network parameters are set to work with your network.
- Initialize the HSM on the Luna SA appliance
- Create and exchange certificates between the Luna SA and your "Client" system (registered the Client with the Partition).
- Create a partition on the HSM and remember the partition password that will be use later.
- Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from Luna SA. The general form of command is “C:\Program Files\SafeNet\LunaClient\vtl verify”.
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Lieberman ERPM Setup

Lieberman ERPM must be installed on the target machine to carry on with the integration process.

The following setup is required:

- A Windows Server 2012 R2 machine.

The installation of ERPM or RPM is addressed in the installation guide which may be downloaded from the documentation section on Lieberman Software's website at

http://www.liebsoft.com/Support_Documentation

The installation guide also covers port requirements and supported host operating systems as well as the installation of pre-requisites such as IIS, MS SQL, accounts, and more.

CHAPTER 2
Integrating Lieberman ERPM with Luna HSM

This chapter outlines the steps to create encryption keys which are secured on Luna HSM.

Configuring the ERPM to use keys from Luna HSM

a) Log on to system as an administrative privilege.

b) Copy the Chrystoki Configration file from following directory:

C:\Program Files\SafeNet\LunaClient\crystoki.ini

To

C:\Program Files\SafeNet\LunaClient\win32\crystoki.ini

c) Edit the configuration file “C:\Program Files\SafeNet\LunaClient\win32\crystoki.ini” and make the following changes in [Chrystoki2] section:

[Chrystoki2]

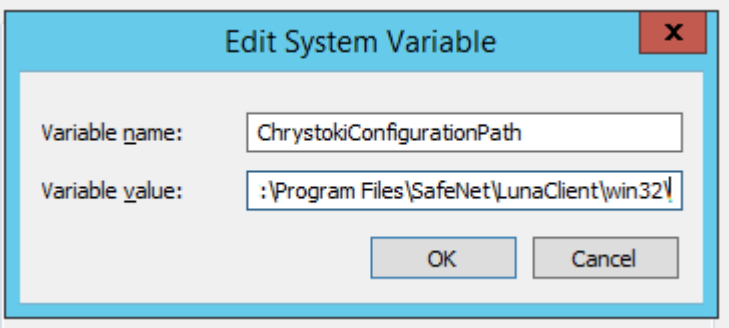
LibNT=C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll

d) To use the 32 bit library you need to change ChrytokiConfigurationPath variable, click Start -> System -> Change Settings -> Advanced -> Environment Variables…

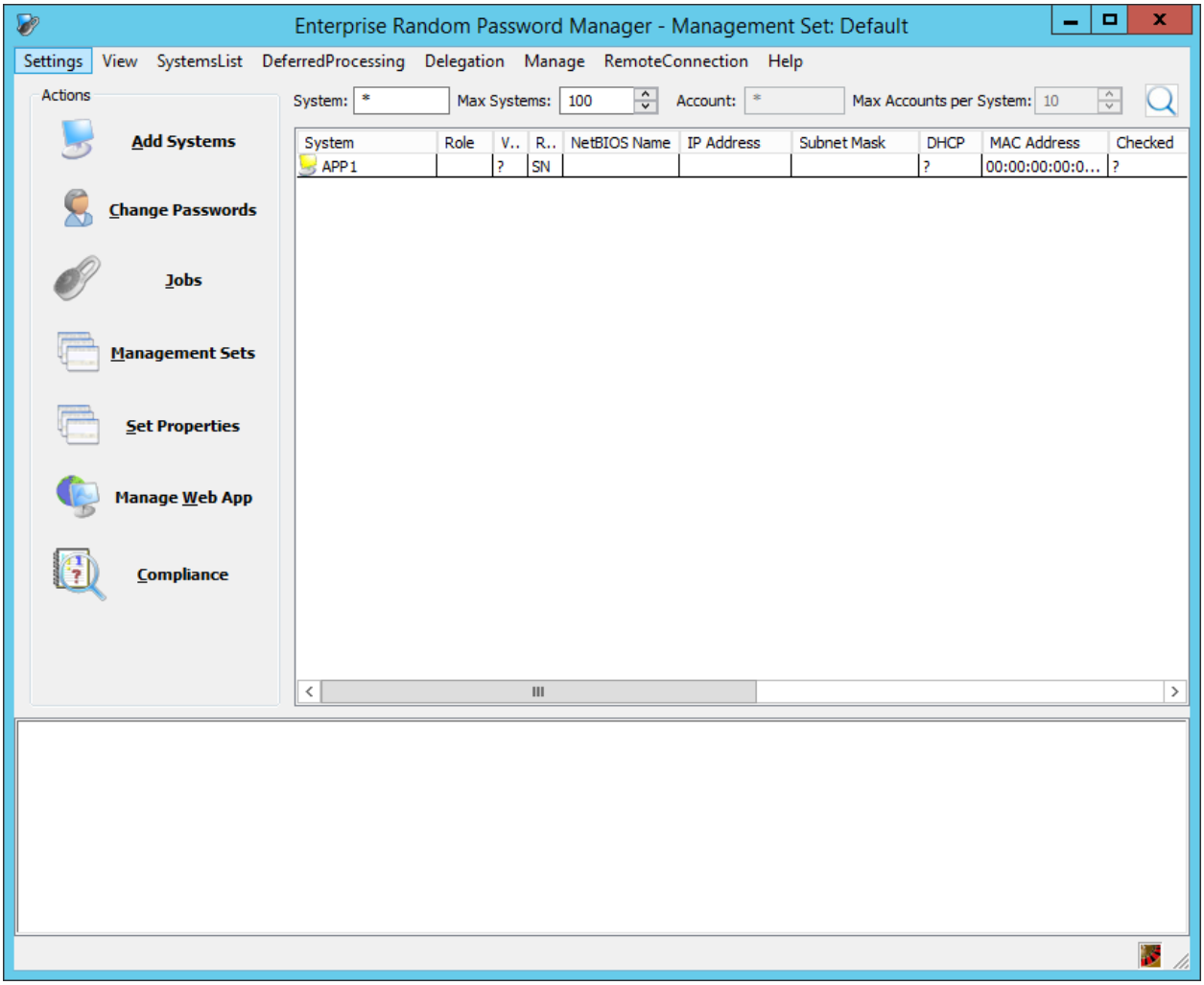
e) Under System Variables, select ChrystokiConfigurationPath, click Edit and set the Variable Value as

“C:\Program Files\SafeNet\LunaClient\win32\”

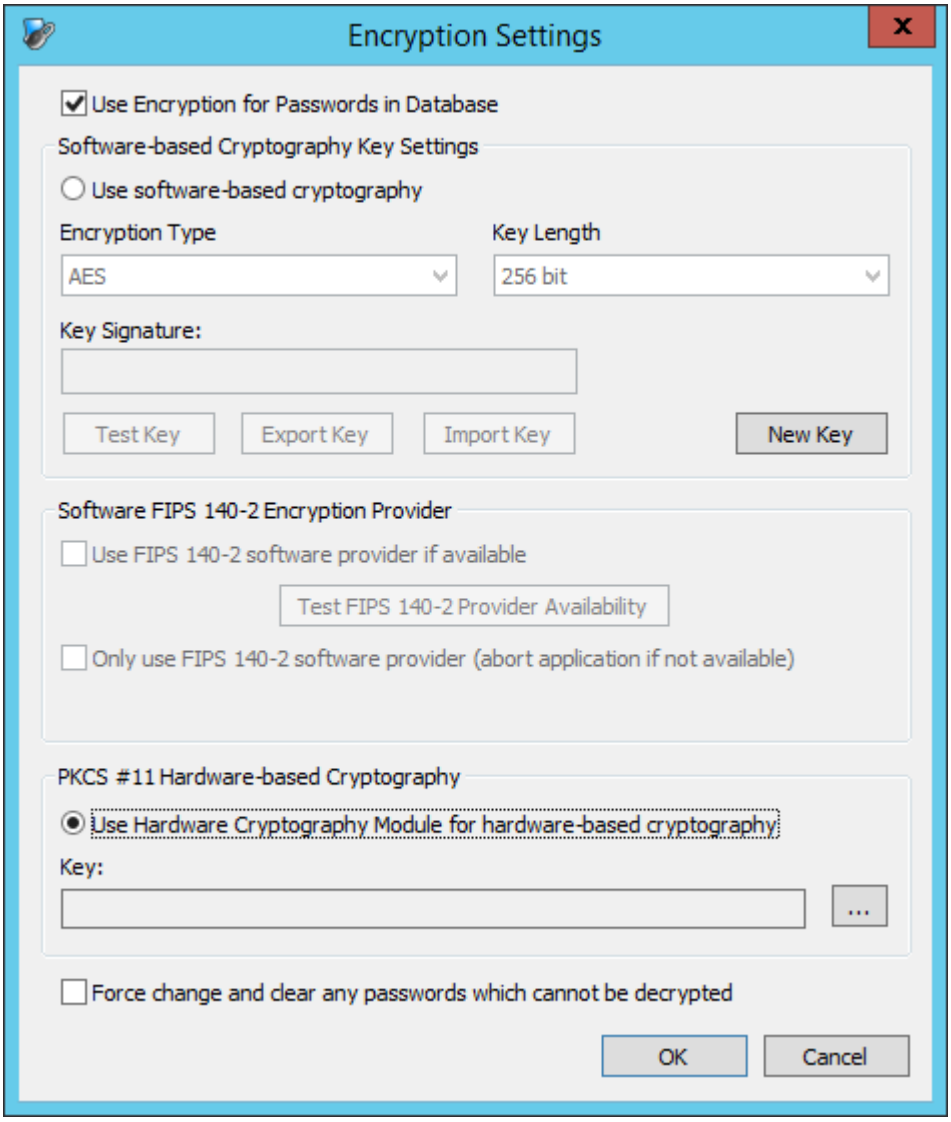
Click OK three times and close the System window.



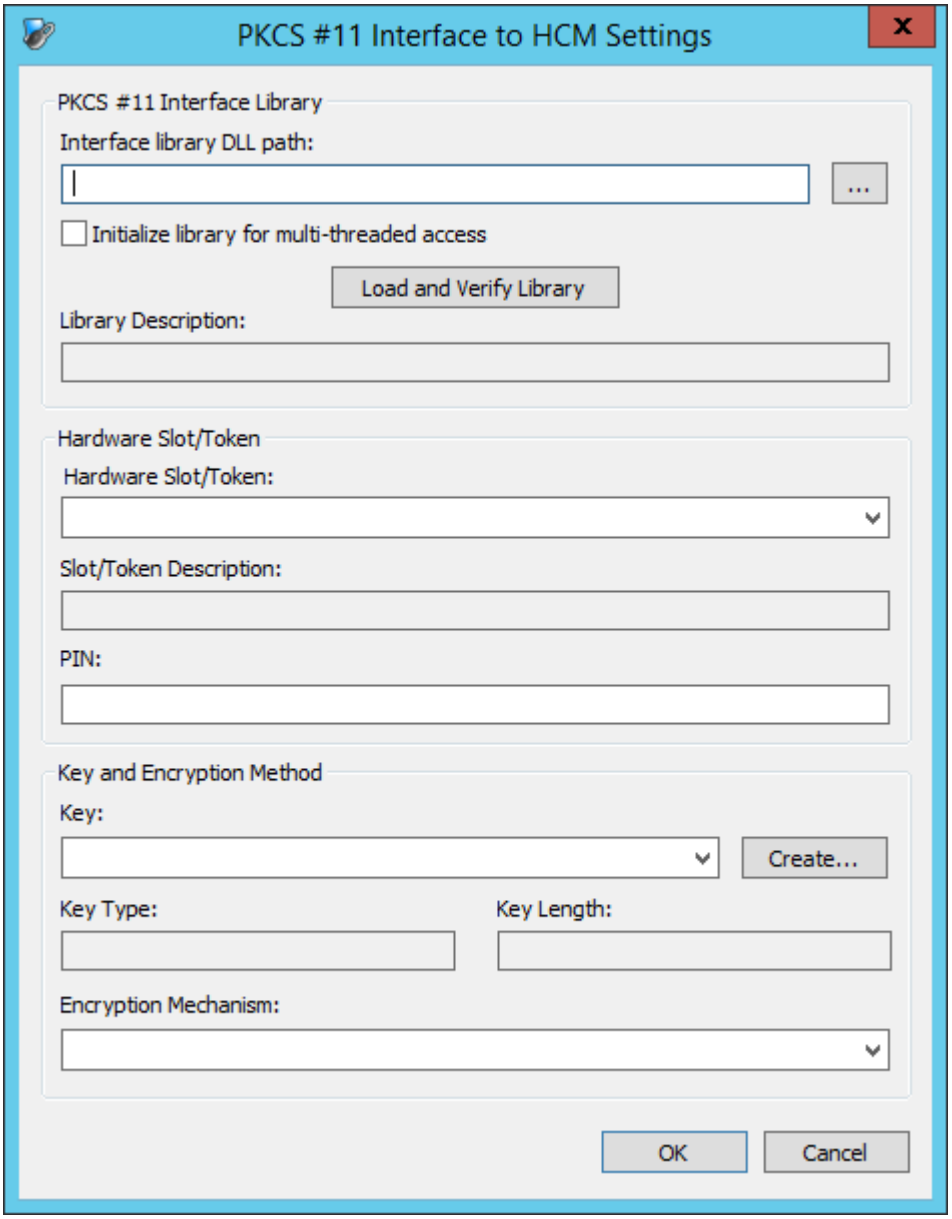
f) Open the ERPM Management Console and click Settings and select Encryption Settings…



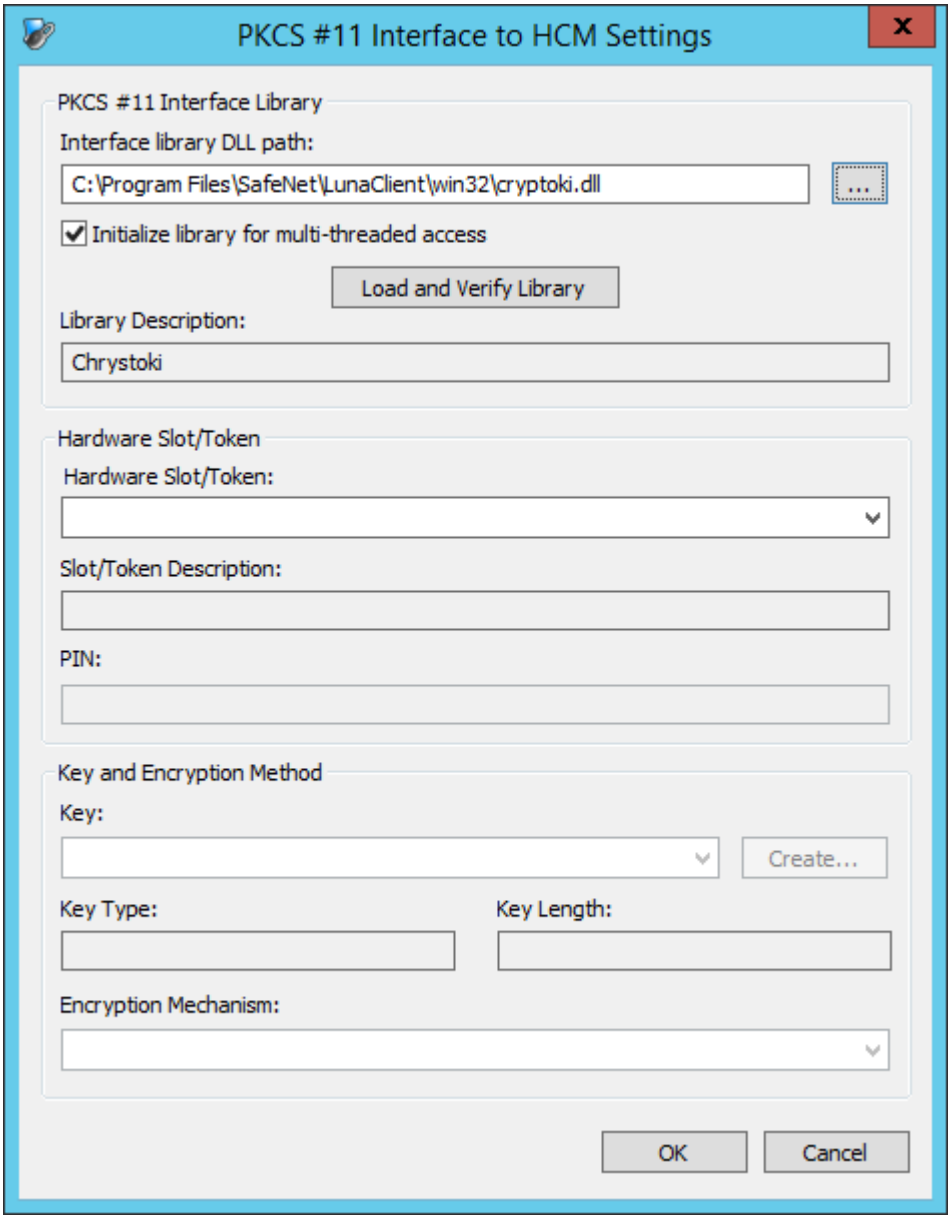
g) In Encryption Settings window, click Use Encryption for Passwords in Database and select Use Hardware Cryptography Module for hardware-based cryptography.



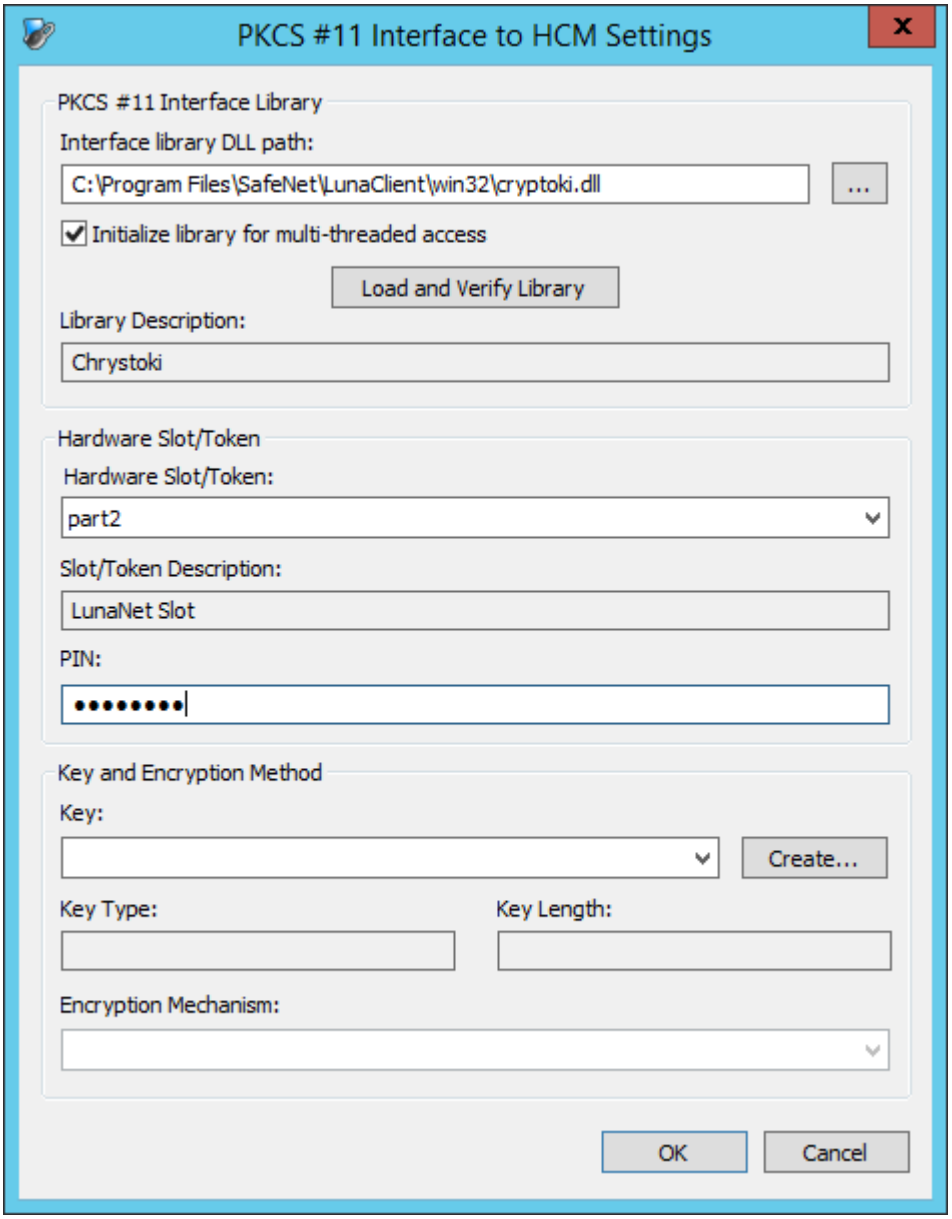
h) Click … button to open the PKCS #11 Interface to HCM Settings console.



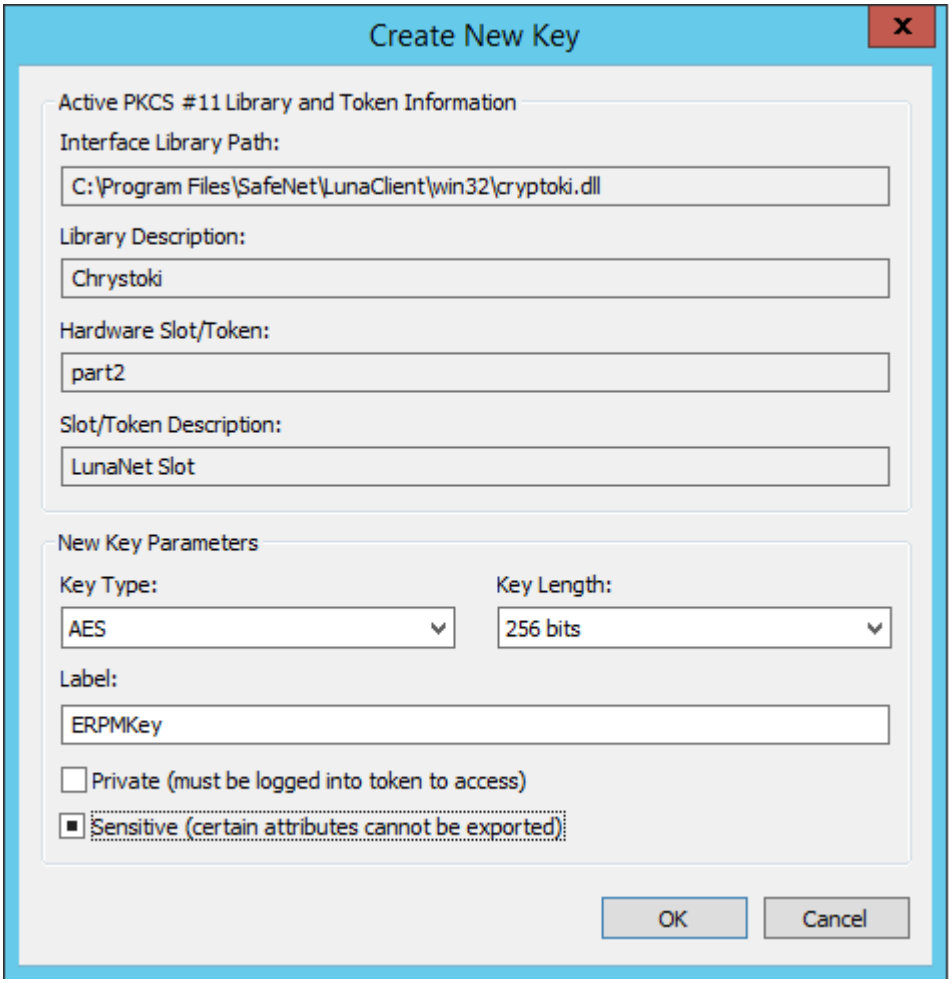
i) Click … button to browse and select C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll library. Select Initialize library for multi-threaded access, click Yes when warning message displayed. After this click Load and Verify Library and click OK.



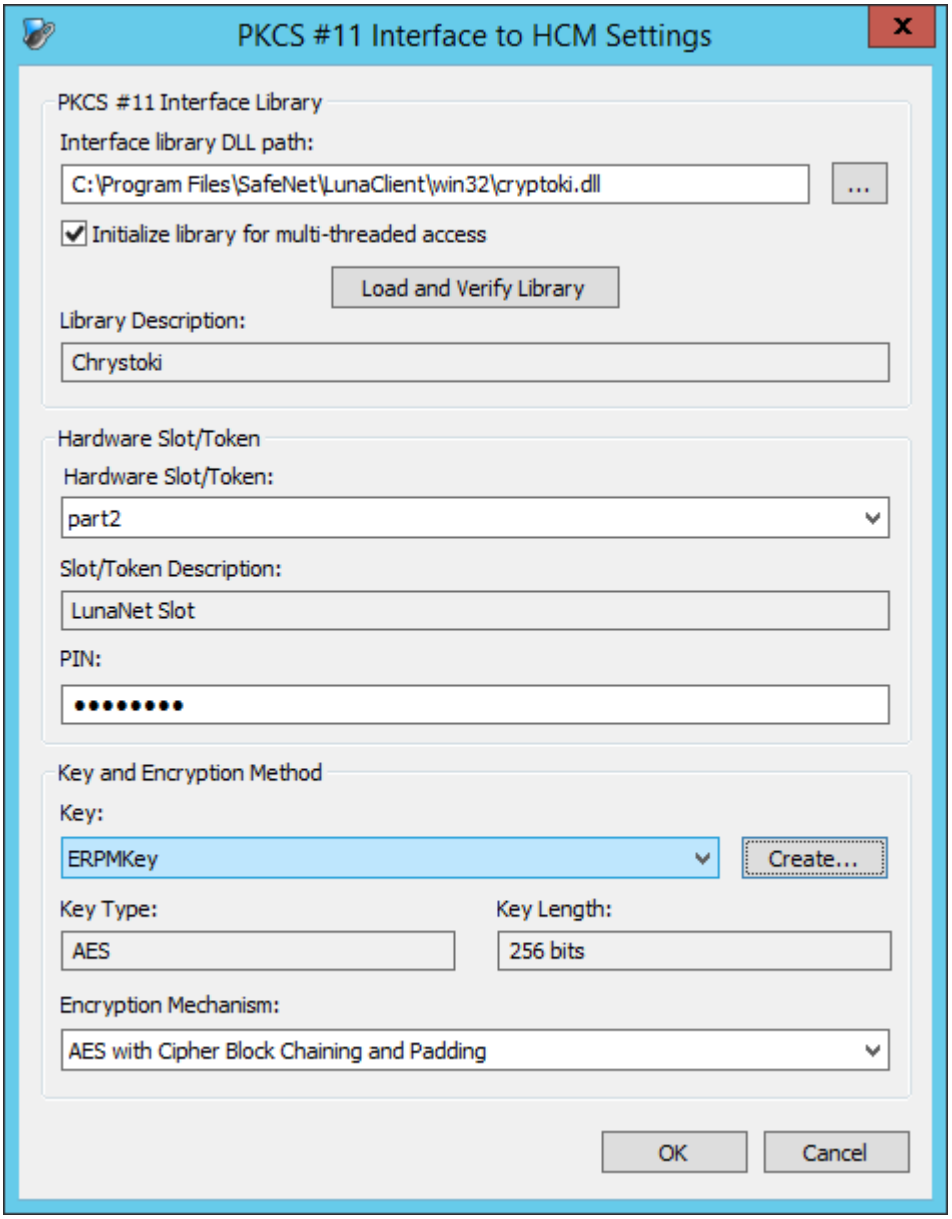
j) Select Hardware Slot\Token and enter the PIN. The PIN will be your HSM partition password.



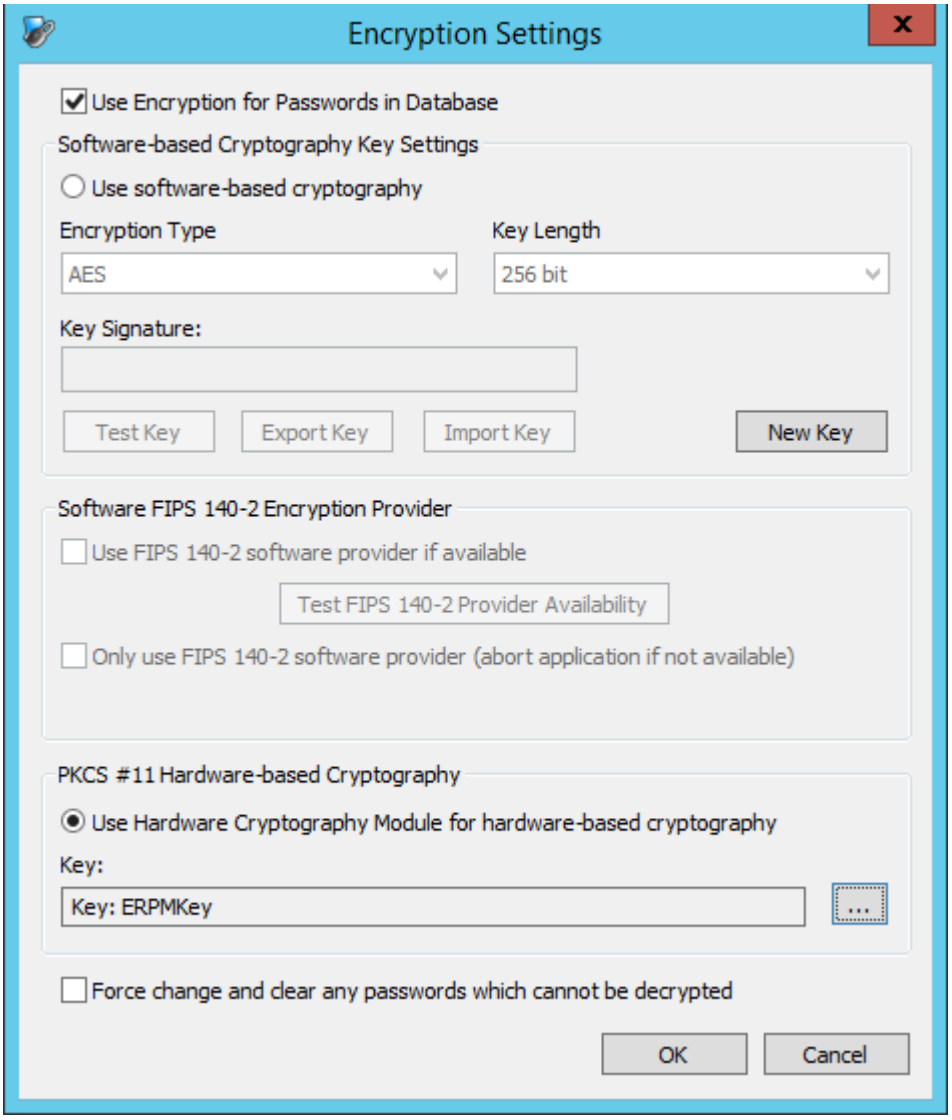
k) Click Create… button, Select Key Type as AES and Key Length as 256 bits and enter the Key Label. Do not select the Private (must be logged into token to access), remove the selection if already selected. Click OK.



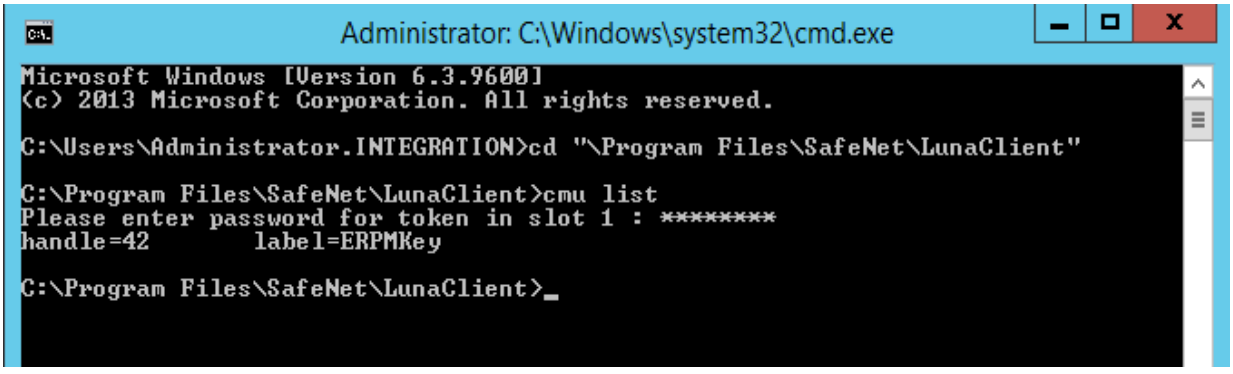
l) Click OK to close the PKCS #11 Interface to HCM Settings console when the key is created.



m) Click OK to close the Encryption Setting console.



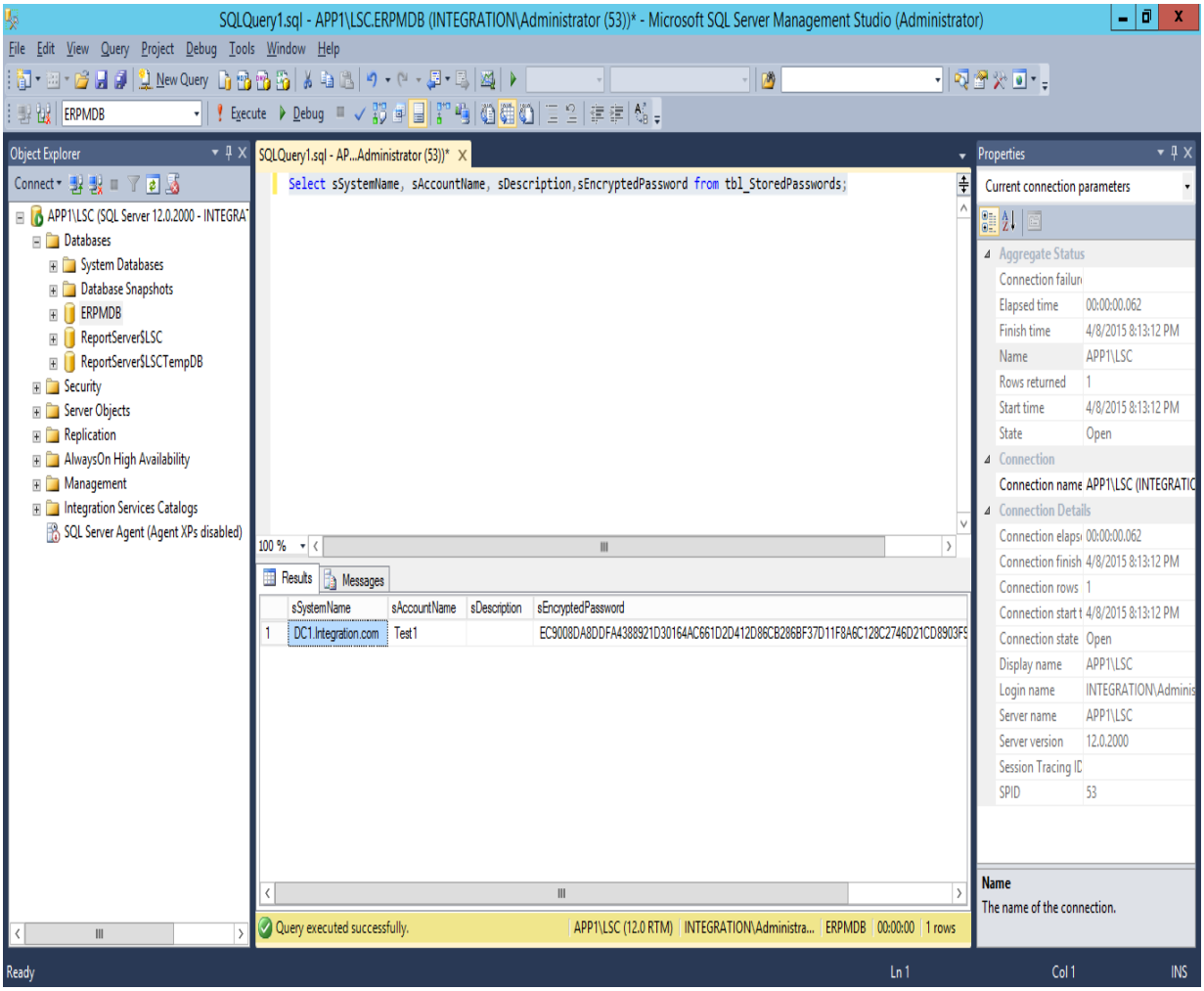
n) You can see the AES key created on the HSM using the CMU utility provided with the client.



ERPMKey created on the Luna SA partition will be used to encrypt all passwords stored in the database and you cannot able to recover the password if the key is lost or HSM is not available.

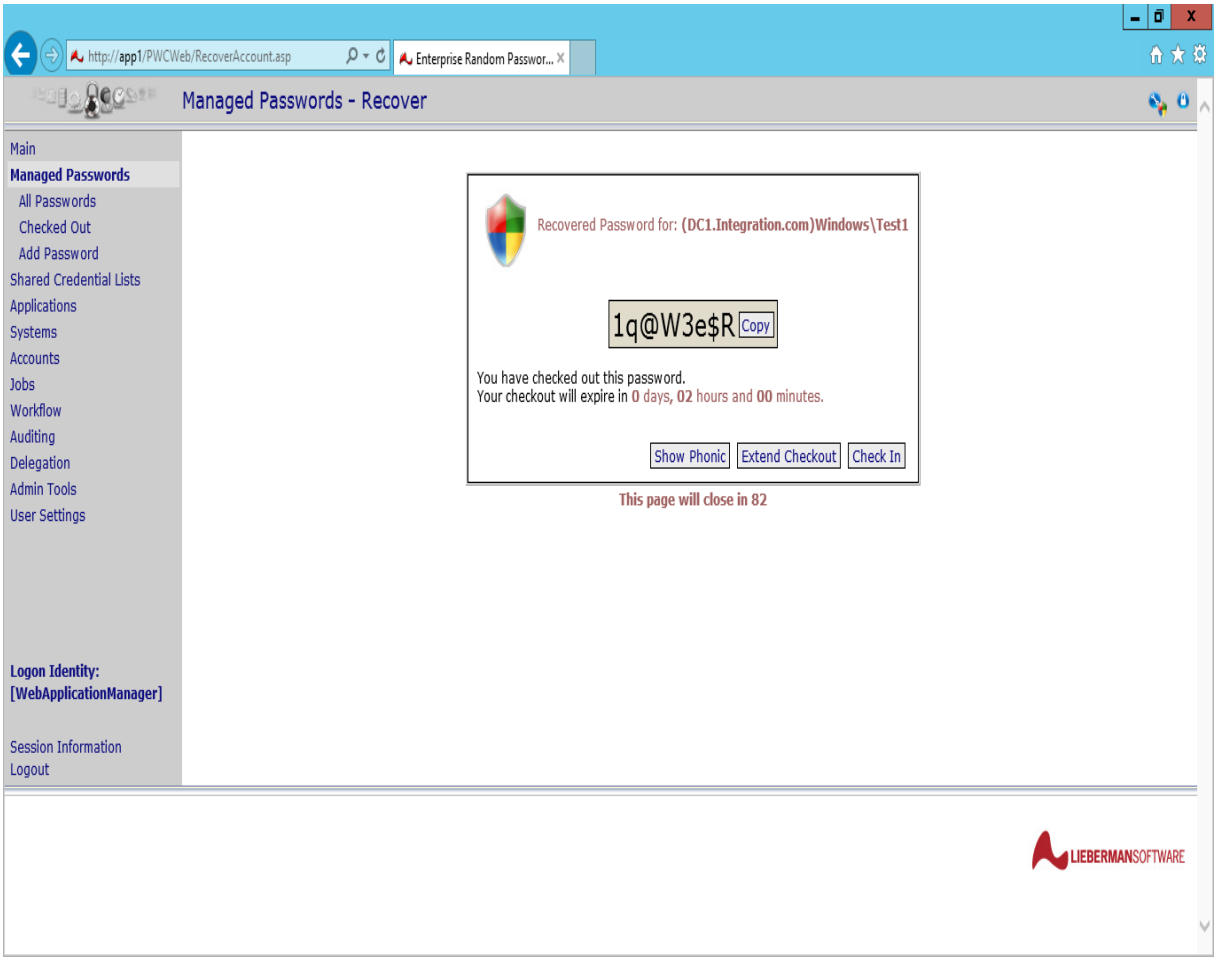
o) You can add the systems in ERPM Management Console and their passwords will be saved in database encrypted using the key created on Luna SA. You can check the Stored Passwords using SQL query below:

```
Select sSystemName, sAccountName, sDescription,sEncryptedPassword from
tbl_StoredPasswords;
```



You can see that password is encrypted using the ERPMKey.

p) To recover the password launch the web console and when logged click on Manage Password -> Options -> Recover Password. Enter the reason for recovery and click Recover. It will display the clear text password after decrypting the encrypted password stored in database using ERPMKey created on Luna SA.



It shows that we can recover the password only if the ERPMKey created on the Luna SA partition is available. We can see that Integration is completed and working as expected.