
SCOM/SCCM Management Pack Installation Guide

Contents

Copyright Notice 2

Overview	1
License Agreement.....	2
Limited Warranty	3
Background and Goals	4

Pre-Requisites 5

Installation 6

Basic Installation	7
SCCM Management Pack Install	7
SCOM Management Pack Install.....	12
Configuration	17
Import the Management Pack	21
SCCM Management Pack Import.....	21
SCOM Management Pack Import.....	21

Index 26

Copyright Notice

Copyright © 2003-2009 Lieberman Software Corporation.
All rights reserved.

The software contains proprietary information of Lieberman Software Corporation; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Lieberman Software and the client and remains the exclusive property of Lieberman Software. If there are any problems in the documentation, please report them to Lieberman Software in writing. Lieberman Software does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Lieberman Software.

Microsoft, Windows, Word, Office, SQL Server, SQL Express, Access, MSDE, and MS-DOS are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.



Lieberman Software Corporation
1900 Avenue of the Stars
Suite 425
Los Angeles
CA 90067
310.550.8575

Internet E-Mail: support@liebsoft.com
Website: <http://www.liebsoft.com>

Lieberman Software has provided add-ons for its Enterprise Random Password Manager and Random Password Manager products to provide integrations into Microsoft's System Center Operations Manager and Configuration Manager products.

In This Chapter

Overview	1
License Agreement	2
Limited Warranty.....	3
Background and Goals.....	4

Overview

Lieberman Software has provided Management Packs for use with Random Password Manager and Enterprise Random Password Manager and Microsoft System Center Operations Manager (SCOM) and Microsoft System Center Configuration Manager (SCCM).

Random Password Manager is designed to randomize and store the passwords for accounts on target systems on a regular recurring basis. Because these passwords are stored and managed by the program, they can be retrieved via a delegated web interface. Access to the password store as well as other web interface features can be limited to specific Windows groups, Windows users, or explicit accounts.

Enterprise Random Password Manager builds on this concept by automatically discovering all references to the specified account, such as services, tasks, COM and D/COM objects, and more, and following a password change for a users account, whether domain or local, propagating the new password to all those references.

License Agreement

This is a legal and binding contract between you, the end user, and Lieberman Software Corporation. By using this software, you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, you should return the software and documentation, as well as, all accompanying items promptly for a refund.

1. Your Rights: Lieberman Software hereby grants you the right to use the Management Packs for Microsoft SCOM and SCCM for Enterprise Random Password Manager or Random Password Manager to manage the licensed number of systems purchased. This software is licensed for use by a single client and its designated employees, contractors and authorized 3rd parties to manage the systems owned/used by a single client. The software license may not be shared with unrelated 3rd parties.

The serial number provided by Lieberman Software is designed for installation on a specific machine. You may install an unlimited number of copies of Enterprise Random Password Manager or Random Password Manager for your administrators that connect to the single licensed machine. All administrators can share the pool of purchased managed node licenses.

There are no limits to the number of web servers or clients that may access the data stored by your licensed copy of Enterprise Random Password Manager or Random Password Manager.

The cost of Microsoft web servers, SSL certificates, and other supporting equipment and technology are the sole responsibility of the user of this software; not Lieberman Software.

2. Copyright. The SOFTWARE is owned by Lieberman Software and is protected by United States copyright law and international treaty provisions. Therefore, you must treat the software like any other copyrighted material (e.g. a book or musical recording) except that you may either (a) make one copy of the SOFTWARE solely for backup and archival purposes, or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for backup and archival purposes. The manual is a copyrighted work also--you may not make copies of the manual for any purpose other than the use of the software.

3. Other Restrictions: You may not rent, lease, or transfer the SOFTWARE to any other entity. You may not reverse engineer, de-compile, or disassemble the SOFTWARE that is provided solely as executable programs (EXE files). If the SOFTWARE is an update, any transfer must include the update and all prior versions.

4. Notice: This software contains functionality designed to periodically notify Lieberman Software of demo usage and of the detection of suspected pirated license keys. By using this software, you consent to allow the software to send information to Lieberman Software under these circumstances, and you agree to not hold Lieberman Software responsible for the use of any or all of the information by Lieberman Software or any third party.

When used lawfully, this software periodically transmits to us the serial number and network identification information of the machine running the software. No personally identifiable information or usage details are transmitted to us in this case. The program does not contain any spyware or remote control functionality that may be activated remotely by us or any other 3rd party.



Lieberman Software Corporation
1900 Avenue of the Stars
Suite 425
Los Angeles
CA 90067
310.550.8575
Internet E-Mail: support@liebsoft.com
Website: <http://www.liebsoft.com>

Limited Warranty

The media (optional) and manual that make up this software are warranted by Lieberman Software Corporation to be free of defects in materials and workmanship for a period of 30-days from the date of your purchase. If you notify us within the warranty period of such defects in material and workmanship, we will replace the defective manual or media.

The sole remedy for breach of this warranty is limited to replacement of defective materials and/or refund of purchase price and does not include any other kinds of damages.

Apart from the foregoing limited warranty, the software programs are provided "AS-IS", without warranty of any kind, either expressed or implied. The entire risk as to the performance of the programs is with the purchaser. Lieberman Software does not warrant that the operation will be uninterrupted or error-free. Lieberman Software assumes no responsibility or liability of any kind for errors in the programs or documentation of/for consequences of any such errors.

This agreement is governed by the laws of the State of California.

Should you have any questions concerning this Agreement, or if you wish to contact Lieberman Software, please write:

Lieberman Software Corporation
1900 Avenue of the Stars
Suite 425
Los Angeles
CA 90067

You can also keep up to date on the latest upgrades via our website at <http://www.liebsoft.com> or e-mail us at: sales@liebsoft.com.

Background and Goals

The Need for Strong Local Credentials

Organizations with a need for the most basic access security should use unique local logon credentials customized for each workstation and server in their environment. Unfortunately, most organizations use common credentials (same user name and password for the built-in administrator account) for each system for the ease of creating and managing those systems by the IT Department without any concern as to the consequences to the organization should these common credentials be compromised.

Creating Strong Local Credentials

Lieberman Software's program: ERPM and RPM can change any common account on all workstations and servers in just a few minutes without the need for scripts or any other type of program. The new common credentials can be stored in a local or remote SQL Server database and can be recovered on demand using the password recovery website.

Random Password Manager can be configured to regularly change the passwords of common accounts on all target systems (i.e. workstation built-in administrator account) according to a schedule so that each account receives a fresh cryptographically strong password regularly. This product feature protects the overall security of an organization so that the compromise of a single machine's local administrator password does not lead to the total compromise of the entire organization's security.

Enterprise Random Password Manager builds on this concept by automatically discovering all references to the specified account, such as services, tasks, COM and DCOM objects, and more, and following a password change for a users account, whether domain or local, propagating the new password to all those references.

Monitoring the Password Management Solution

As ERPM and RPM manage and store these credentials a tremendous amount of trust must be placed in ERPM and RPM. The goal of the management pack for SCOM is to provide monitoring and alerting for the components of ERPM and RPM such as the database, deferred processors, application, and web components. The secondary goals for both SCOM and SCCM is to provide a mechanism to recover these stored credentials from a familiar environment.

Pre-Requisites

This manual makes reference to both Random Password Manager (RPM) and Enterprise Random Password Manager (ERPM). The concepts and steps outlined in this manual are applicable to both ERPM and RPM except as where expressly noted.

This section will provide basic instructions to get the management packs for Enterprise Random Password Manager and Random Password Manager for SCOM and SCCM installed and functioning in the shortest amount of time.

In order to perform a successful installation, a few items will be required:

- An installation of ERPM or RPM 4.81 or later
- System Center Operations Manager or System Center Configuration Manager 2007 or later
- The specific URL used by the ERPM or RPM password recovery website
- Network access to the ERPM or RPM password recovery website
- Delegated access to the ERPM or RPM password recovery website
- A local copy of the ERPM or RPM "rouletteclientagentconsole.exe" in a directory of your choosing. This file is found in the installation directory of ERPM or RPM, typically %programfiles%\lieberman\{roulette | rpm} or %programfiles(x86)%\lieberman\{roulette | rpm}
- For SCOM to monitor the application components, each system hosting a component will require the SCOM agent be installed. Please review Microsoft's requirements for installation of the SCOM agent
- Rights to install software on your SCOM/SCCM host system
- Rights to install management packs in your SCOM/SCCM installation

The following sections will outline the requirements and rights required to perform a successful installation of the management packs.

This guide does not cover the installation of Windows, SCOM, SCCM, MS SQL, SCOM and SCCM agents, or ERPM or RPM. This guide assumes that these items are already installed and functioning.

Installation

This section will cover the installation of the management packs, configuration of the management packs, and addition of the management pack to SCOM and SCCM. Examples shows are using Microsoft System Center 2007 editions.

In This Chapter

Basic Installation	7
Configuration.....	17
Import the Management Pack.....	21

Basic Installation

From a machine hosting ERPM/RPM, copy "rouletteclientagentconsole.exe" from the ERPM/RPM installation directory. The installation directory is typically **%programfiles%\lieberman\{roulette | rpm}** or **%programfiles(x86)%\lieberman\{roulette | rpm}**. Create a directory on the SCOM or SCCM host system and copy this one file to this directory. It does not matter what the name of this directory you are creating is called.

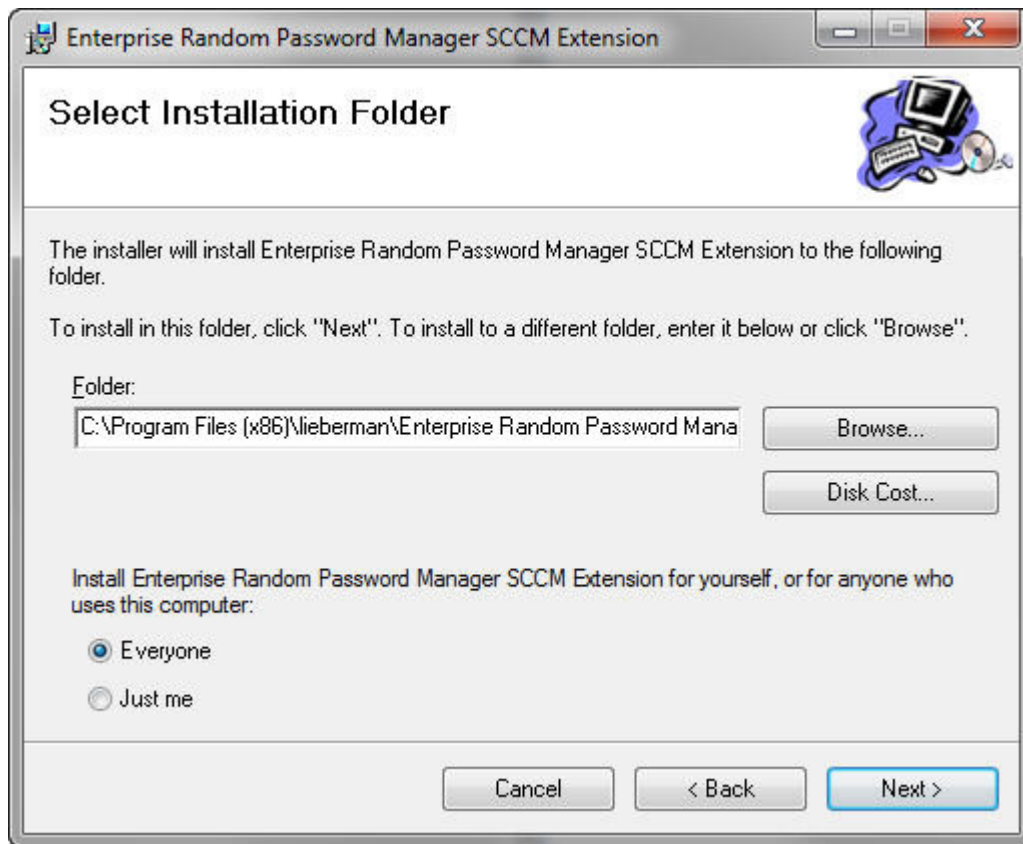
After the file is copied over, begin the installation of the management pack. This will only setup the requisite support files; the management pack will still not be integrated into SCOM/SCCM when this step is complete.

SCCM Management Pack Install

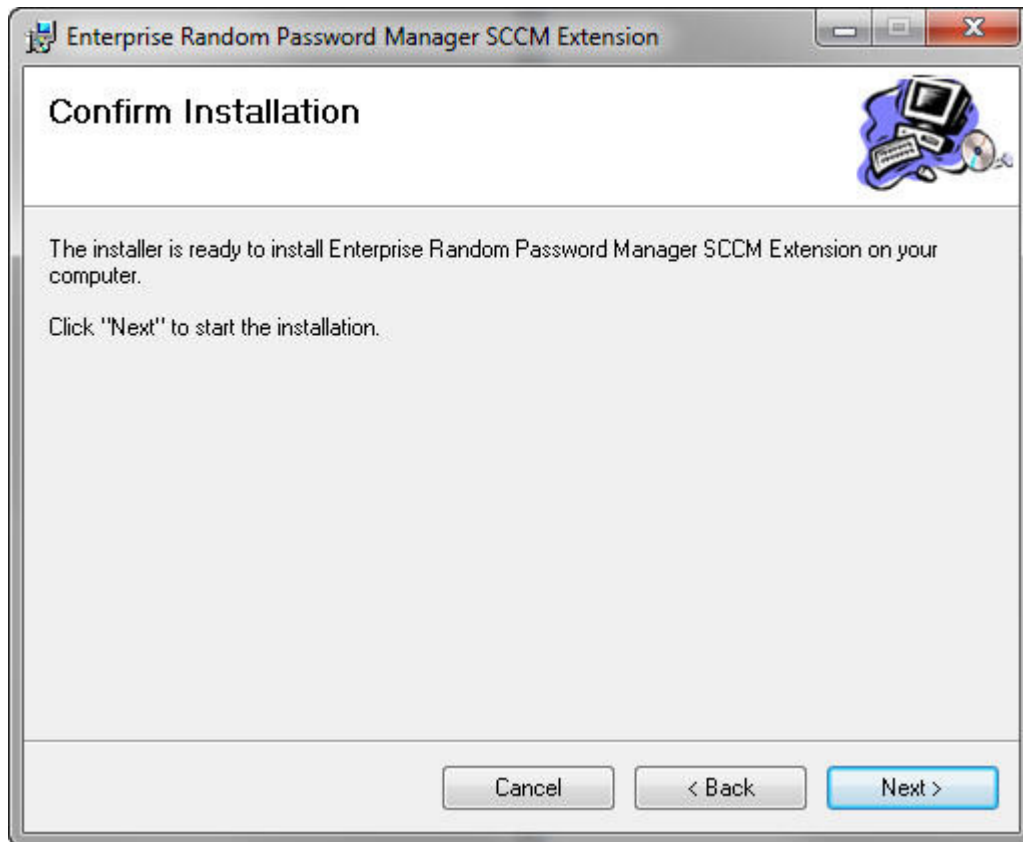
Launch the SCCM Management Pack Installer. Click NEXT to continue.



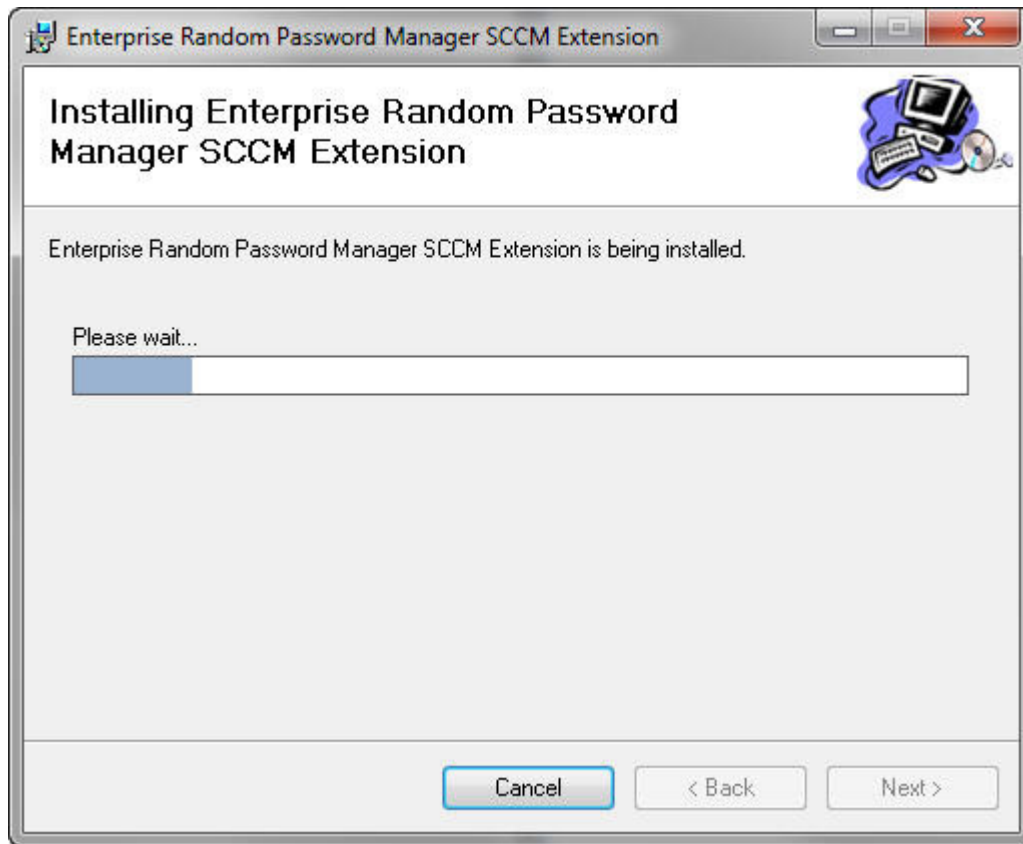
Choose the installation directory for the management pack files. Choose to make the configuration shortcuts available to everyone on the computer or just for you. Click NEXT to continue.



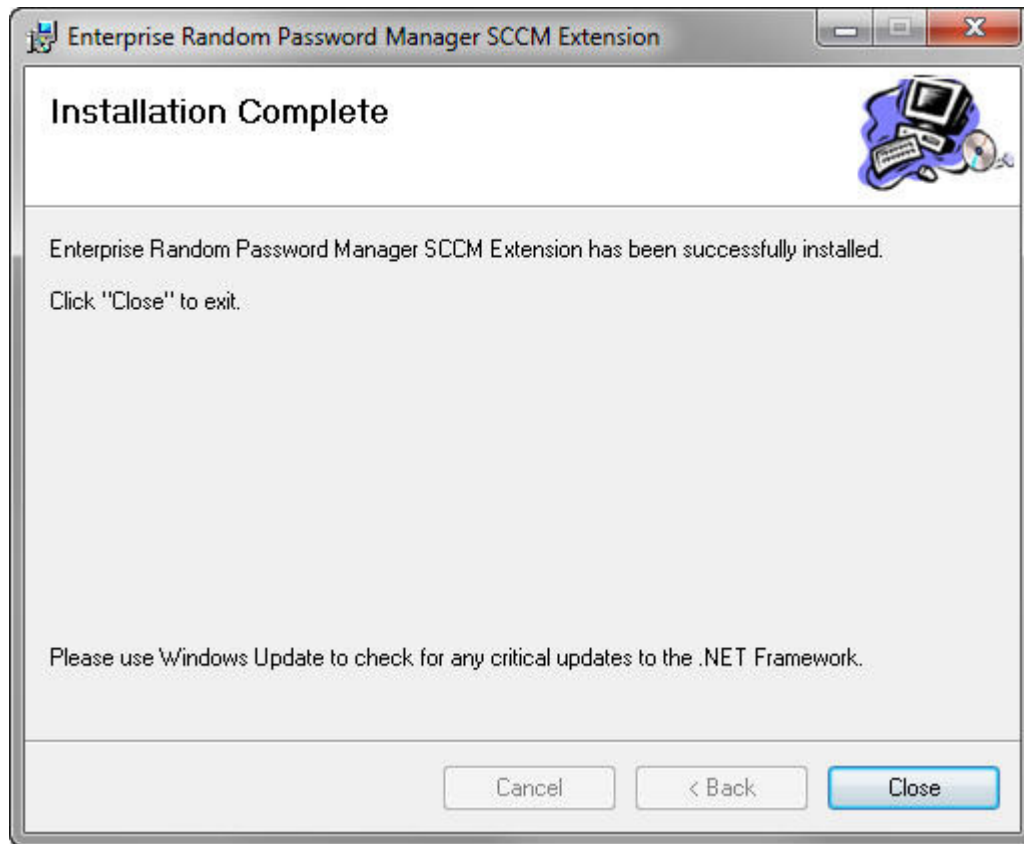
When ready, click NEXT to begin the installation.



Installation of the support files will be quick.



When finished, click CLOSE.



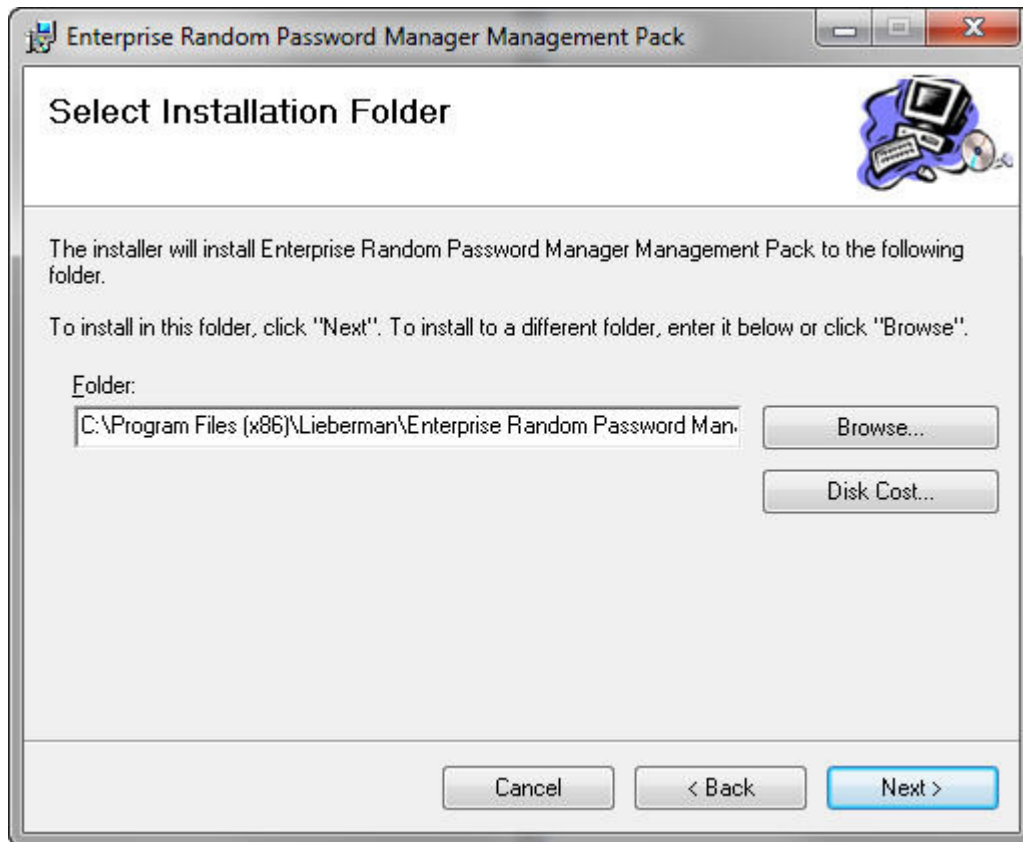
The next step will be to launch the configuration utility from the start menu under "Lieberman Software \ [Enterprise] Random Password Manager Management Pack".

SCOM Management Pack Install

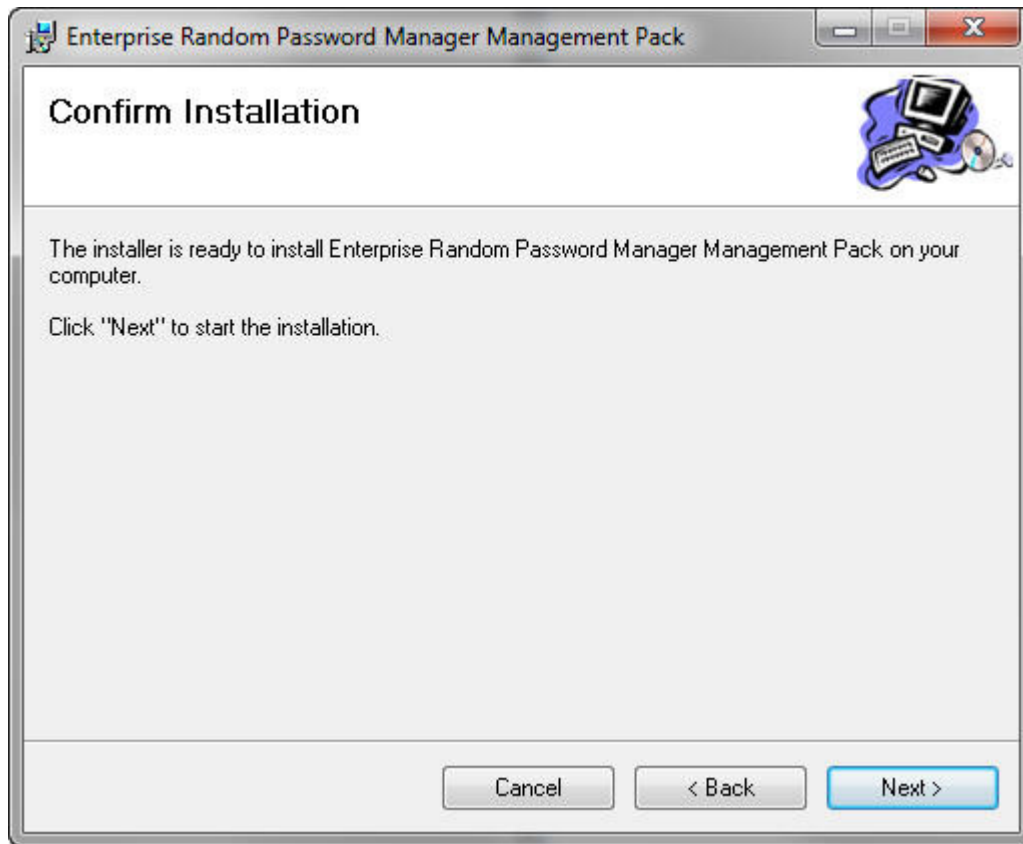
Launch the SCOM Management Pack Installer. Click NEXT to continue.



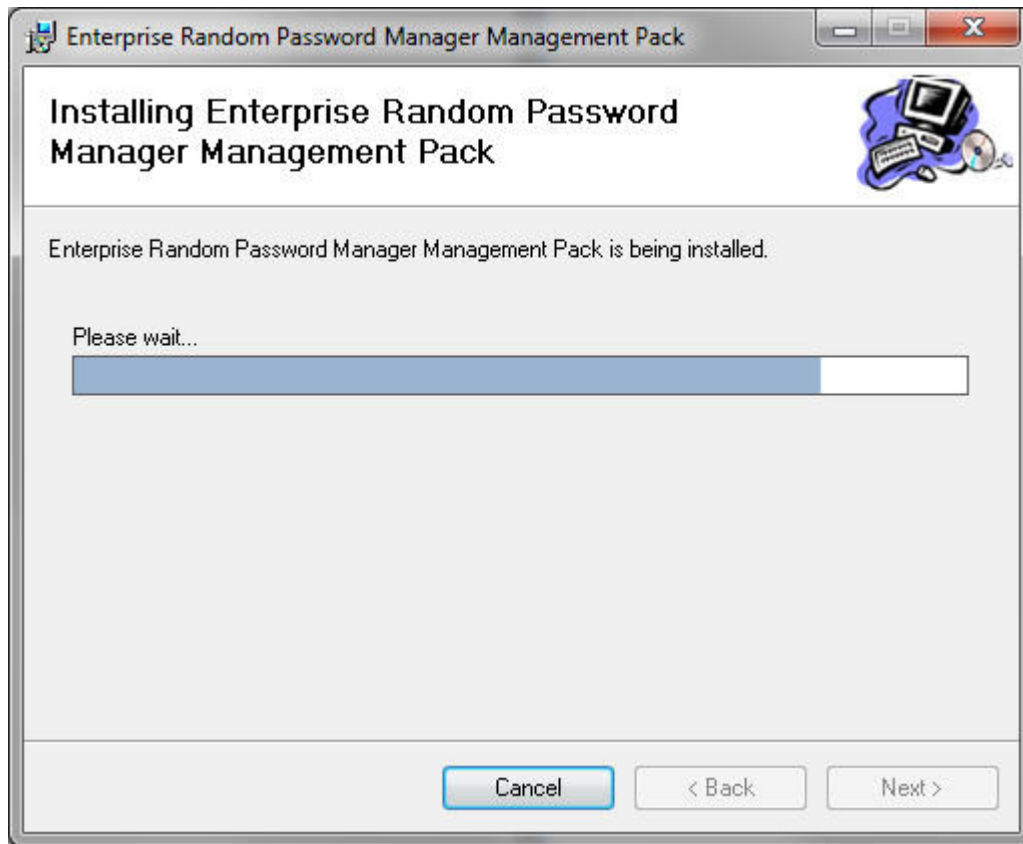
Choose the installation directory for the management pack files. Click NEXT to continue.



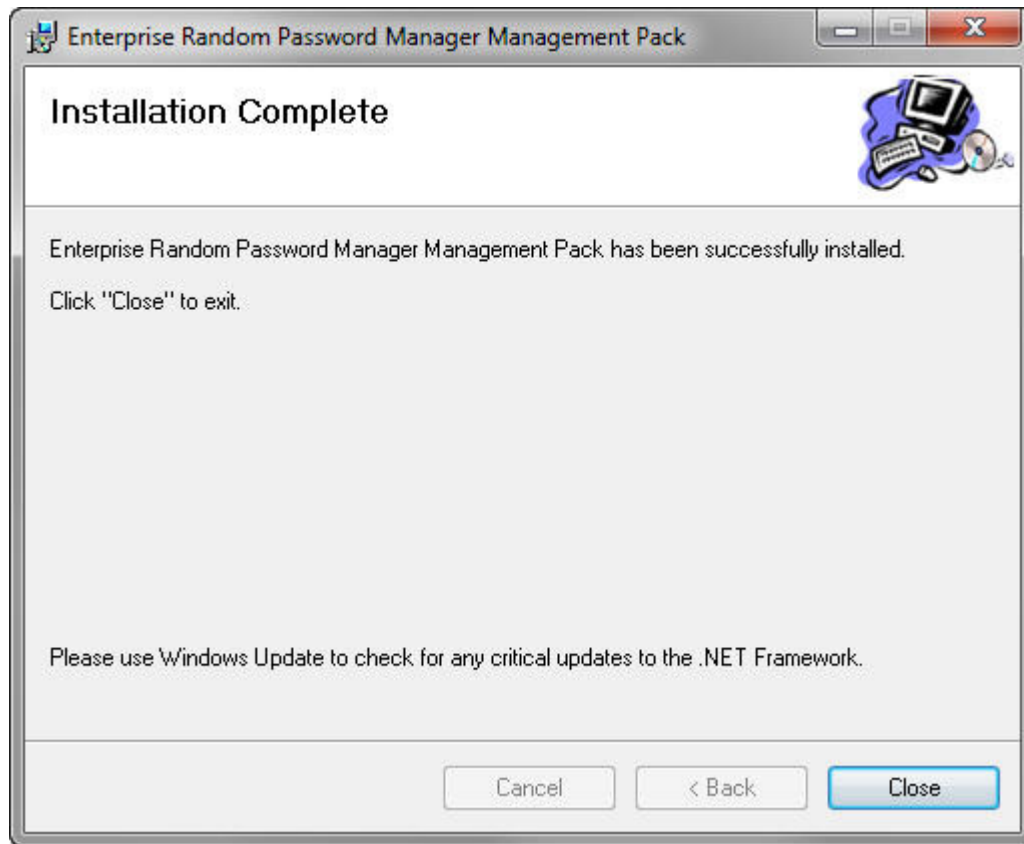
When ready, click NEXT to begin the installation.



Installation of the support files will be quick.



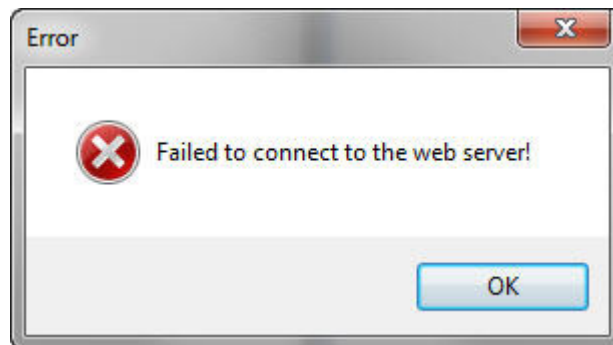
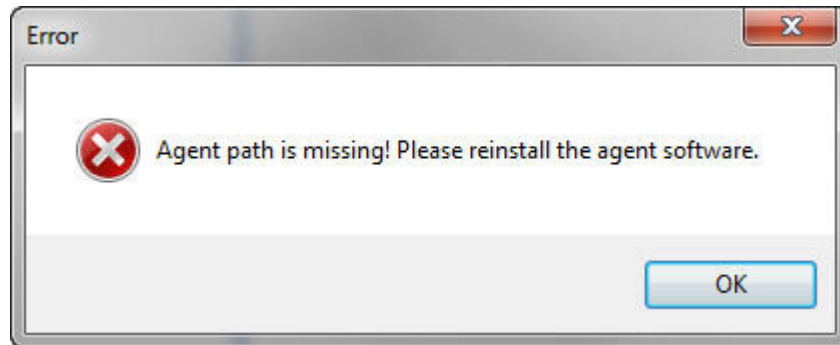
When finished, click CLOSE.



The configuration utility should now launch automatically. If not, it can be launched from the start menu under "Lieberman Software \ [Enterprise] Random Password Manager Management Pack".

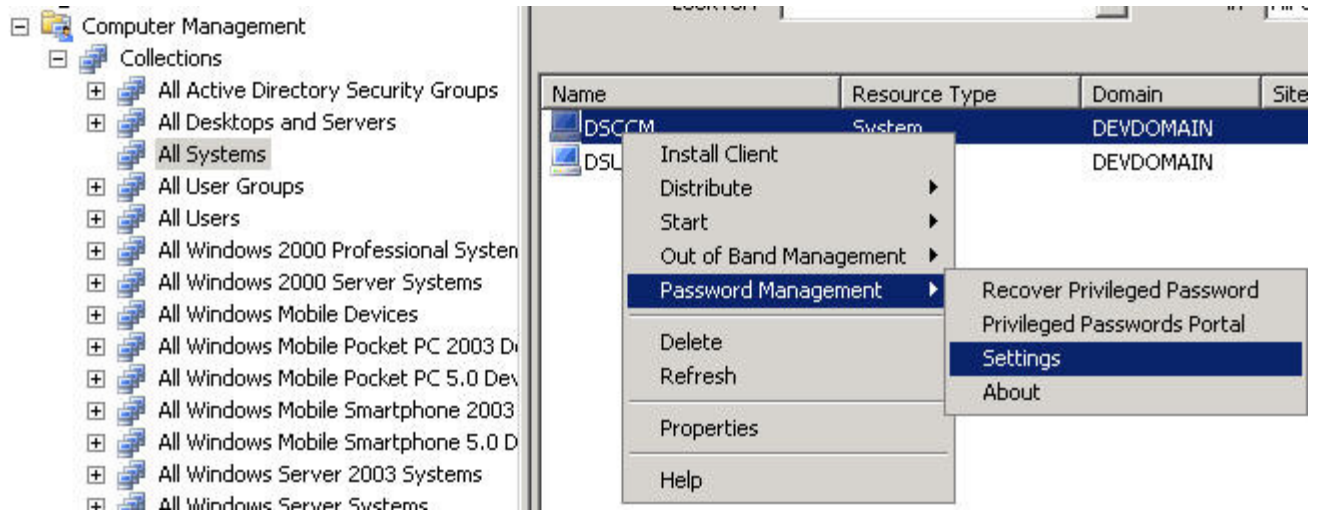
Configuration

If installing the SCOM management pack the configuration utility should launch automatically following installation. If not it can be launched from the start menu under "Lieberman Software \ [Enterprise] Random Password Manager Management Pack". If this is the first time the configuration utility is being launched, a series of errors will appear. These errors can be ignored at this time.

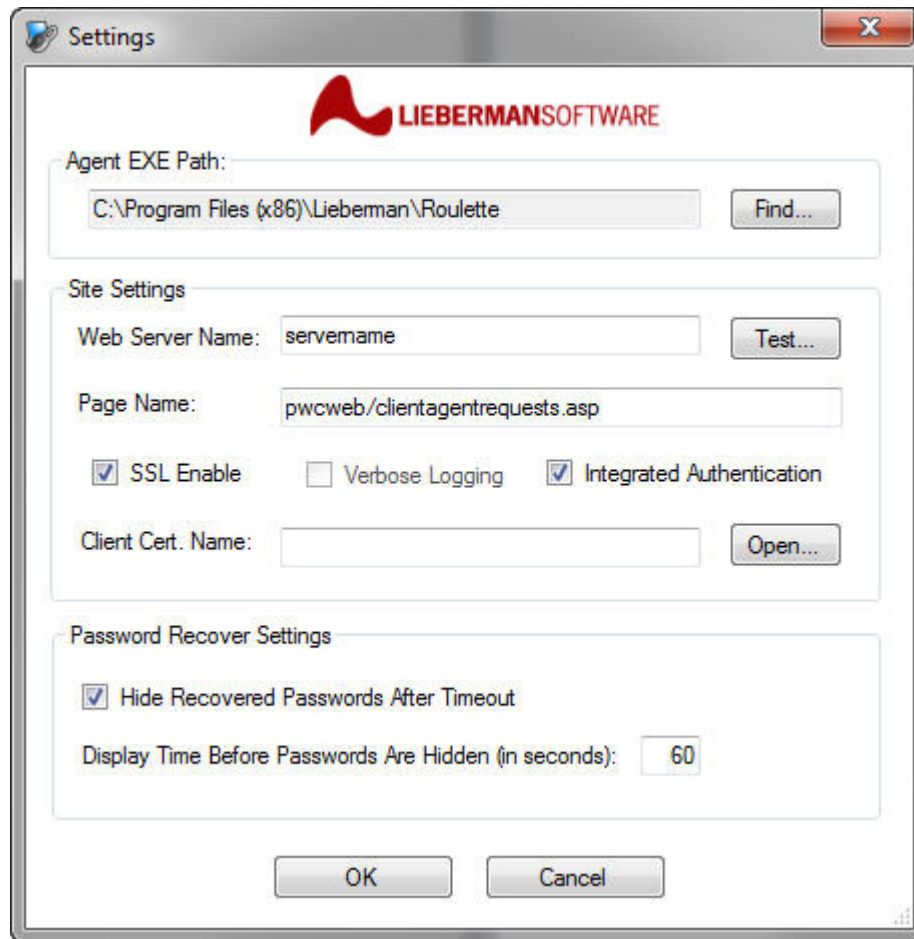


These errors will be rectified by the configurations about to be made.

For SCCM only, the configuration of the management pack occurs from within the SCCM console. Expand 'Site Database\Computer Management\Collections' and choose a system set. Right-click on any system, choose 'Password Management\Settings'.



Once you OK the errors or open the settings item, the configuration dialog will appear.



The screenshot shows a Windows-style dialog box titled "Settings" with a close button (X) in the top right corner. The dialog features the Lieberman Software logo at the top center. It is organized into three main sections: "Agent EXE Path", "Site Settings", and "Password Recover Settings".

Agent EXE Path: This section contains a text input field with the path "C:\Program Files (x86)\Lieberman\Roulette" and a "Find..." button to its right.

Site Settings: This section includes a "Web Server Name" field with the value "servename" and a "Test..." button. Below this is a "Page Name" field with the value "pwcweb/clientagentrequests.asp". There are three checkboxes: "SSL Enable" (checked), "Verbose Logging" (unchecked), and "Integrated Authentication" (checked). At the bottom of this section is a "Client Cert. Name" field and an "Open..." button.

Password Recover Settings: This section has a "Hide Recovered Passwords After Timeout" checkbox (checked) and a "Display Time Before Passwords Are Hidden (in seconds):" field with the value "60".

At the bottom of the dialog are "OK" and "Cancel" buttons.

The items which must be configured in this dialog is:

- Agent EXE Path: This is the path on the local system where "rouletteclientagentconsole.exe" was copied to.
- Web Server Name: This is the short or fully qualified name (used in the URL) of the web server hosting the password recovery website
- Page Name: This is the path on the web server to the "clientagentrequests.asp" page. If the password recovery website was installed to a root directory, simply enter "clientagentrequests.asp" in this field. If the password recovery website was installed to a virtual directory (default) the path for ERPM will typically be "pwcweb/clientagentrequests.asp" while the path for RPM will be "rpmweb/clientagentrequests.asp"
- If SSL is enabled, select the "SSL Enable" check box. The web server or its issuing CA must also be trusted by the host system.
- If integrated authentication has been setup for the password recovery website, leverage this option by selecting the "integrated Authentication" check box. If Integrated authentication is not enabled on the web server do not enable this option.

The final options on this page are to hide the displayed passwords after N number of seconds. This ensures that even if the password is left on display, it will not be indefinitely.

Click OK once all the options are configured. The final step of the installation is performed from within SCOM or SCCM by importing the management pack.

Import the Management Pack

The final step to being able to use the management packs are to import them into SCOM or SCCM. These steps are outlined in the following section.

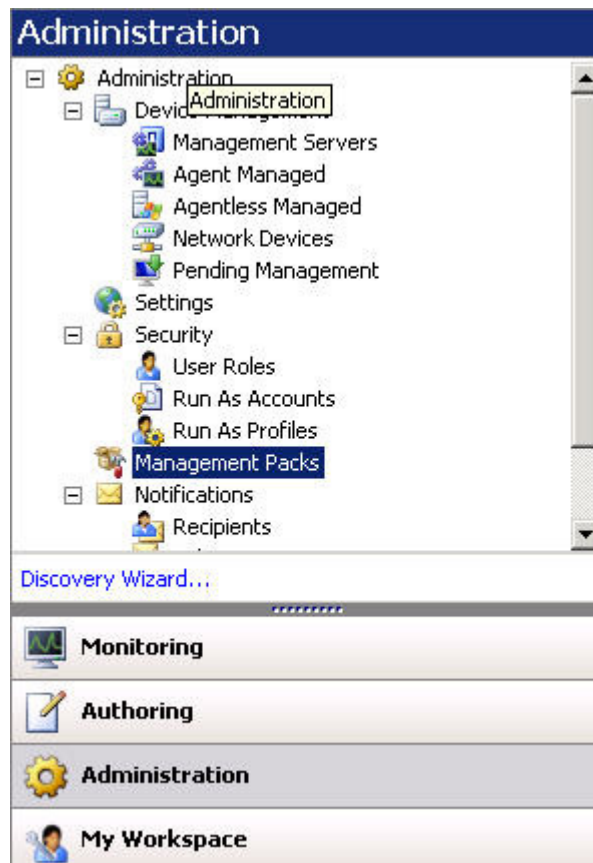
See the Admin Guide for steps on using and leveraging the management packs.

SCCM Management Pack Import

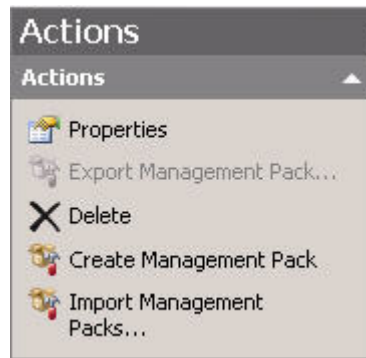
There are no further steps to take in order to make use of the management pack for SCCM. Once the product is installed and configured, it is ready to use. See the admin guide for procedures on using the management pack.

SCOM Management Pack Import

Open The SCOM management console as a user with the rights to install a management pack. On the left pane, select 'Administration'. From the administration pane, select 'Management Packs'.

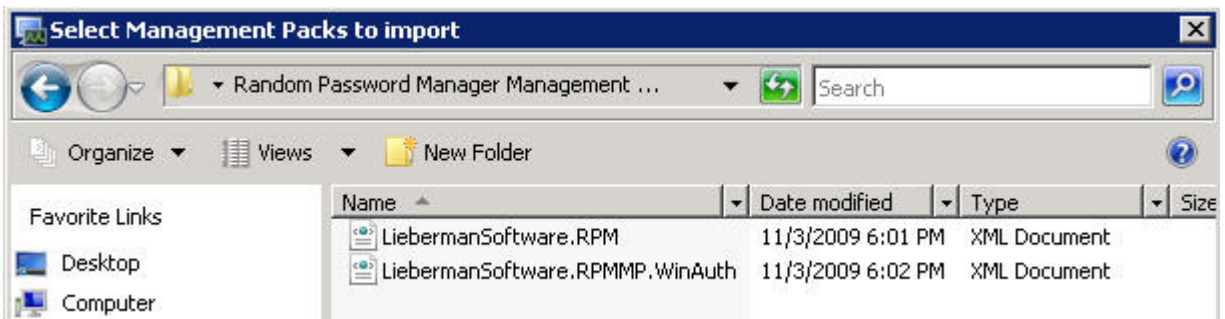


From the top right actions pane, select 'Import Management Packs...'.

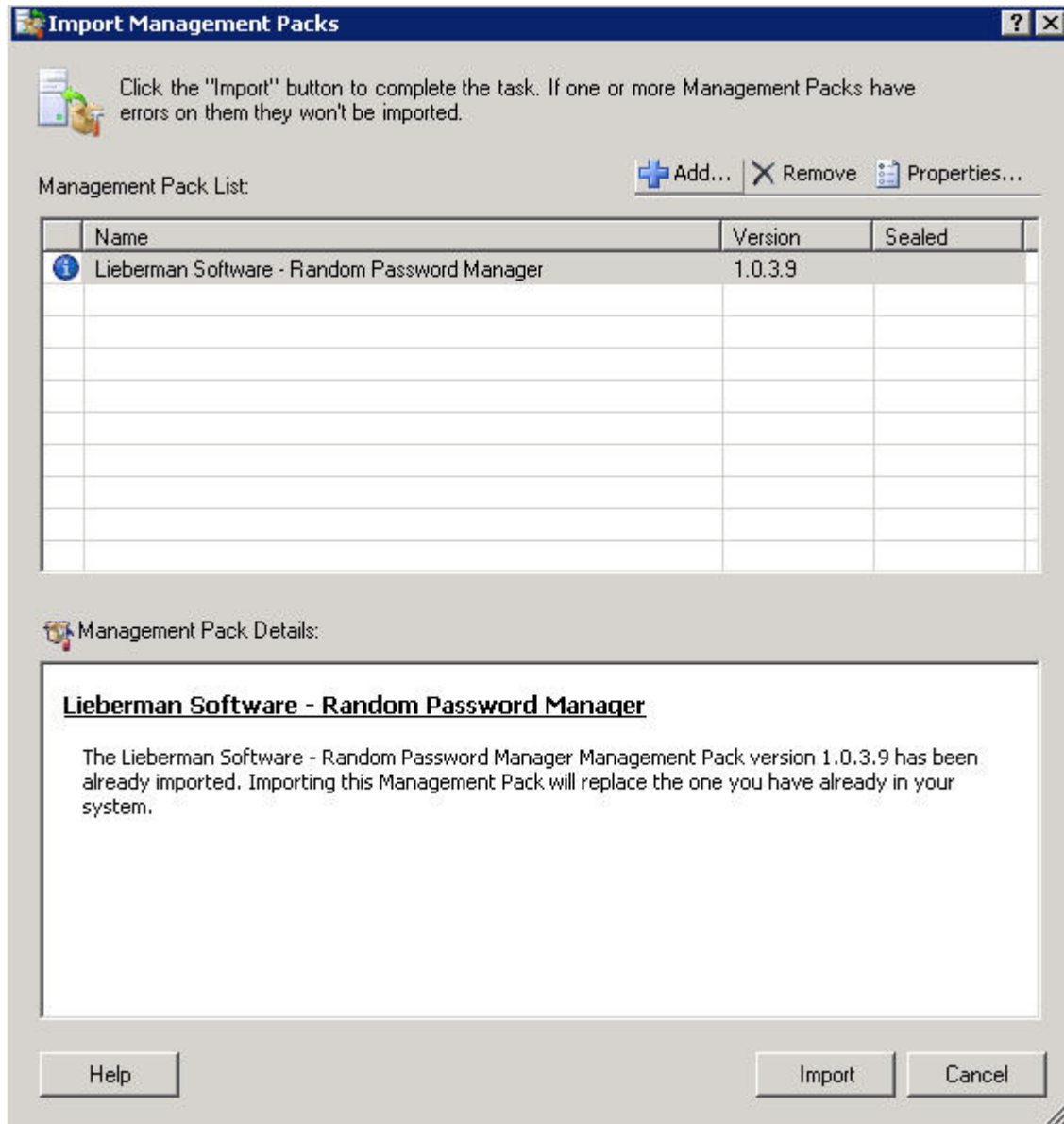


Browse to the folder that the management pack was installed to. By default, this is "%programfiles%\\lieberman\\[Enterprise] Random Password Manager Management Pack" or "%programfiles(x86)%\\lieberman\\[Enterprise] Random Password Manager Management Pack".

When the folder is opened there will be two choices for management pack files to install: one with WinAuth and one without WinAuth. The file with WinAuth will attempt to use integrated authentication to connect to the ERPM/RPM database server. The file without WinAuth will attempt to use explicit SQL authentication to connect to the ERPM/RPM database server. It is recommended when possible to use the WinAuth option. If you must use the non-WinAuth option, you will also be asked for the explicit SQL credentials used to connect to the SQL database.



Once the management pack is selected, click the 'Import' button.



When the management pack is installed, a new node will appear under the monitoring section called "Lieberman Software - [Enterprise] Random Password Manager". This new node will have multiple sub nodes for each component of the product. Under the 'Computers' node in the action pane, you will also find a new task called '[Enterprise] Random Password Manager - Recover Privileged Password'.



Index

B

Background and Goals • 4

Basic Installation • 7

C

Configuration • 17

Copyright Notice • 2

I

Import the Management Pack • 21

Installation • 6

L

License Agreement • 2

Limited Warranty • 3

O

Overview • 1

P

Pre-Requisites • 5

S

SCCM Management Pack Import • 21

SCCM Management Pack Install • 7

SCOM Management Pack Import • 21

SCOM Management Pack Install • 12