SCOM/SCCM Management Pack Admin Guide

Contents

Copyright Notice

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

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 many 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.

Using the Management Packs

SCOM and SCCM serve different roles in an enterprise. SCOM allows for monitoring and reactive management of systems while SCCM allows for proactive management, maintenance, and reporting of managed systems. Lieberman Software has provided management packs to provide further integrations into these Microsoft products for its Enterprise Random Password Manager and Random Password Manager products.

The SCOM integration allows for monitoring of the components of ERPM/RPM such as the database, zone and deferred processors, web instances, and other relevant statistics. Both SCOM and SCCM integration allow for recovery of the managed account's passwords from within the SCOM and SCCM management interfaces.

The following sections outline how to use the management packs to perform their respective duties from within the respective platform.

In This Chapter

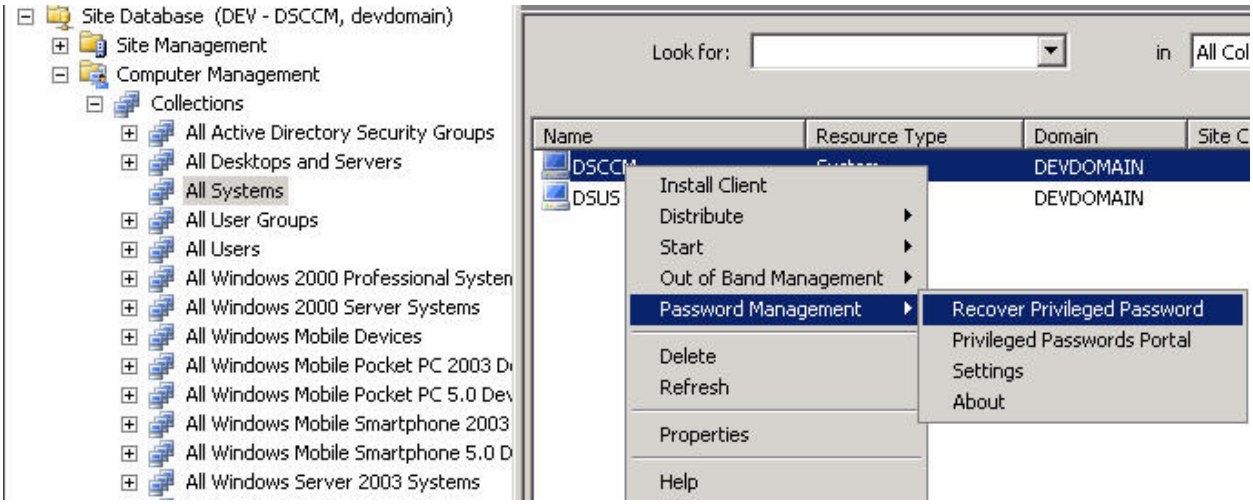
SCCM - Recovering Passwords

In order to be able to recover the password for an account being managed by ERPM/RPM, the system must also appear in the list of managed systems in the SCCM interface. If there are no stored accounts available when you attempt a recovery, you will be notified as such.

There are two possible reasons as to why a message indicating there are no stored accounts may appear:

- There truly are no stored passwords
- The credentials used to login/recover the passwords does not have the ability to see any accounts on the selected system - see the ERPM/RPM web delegation rules.

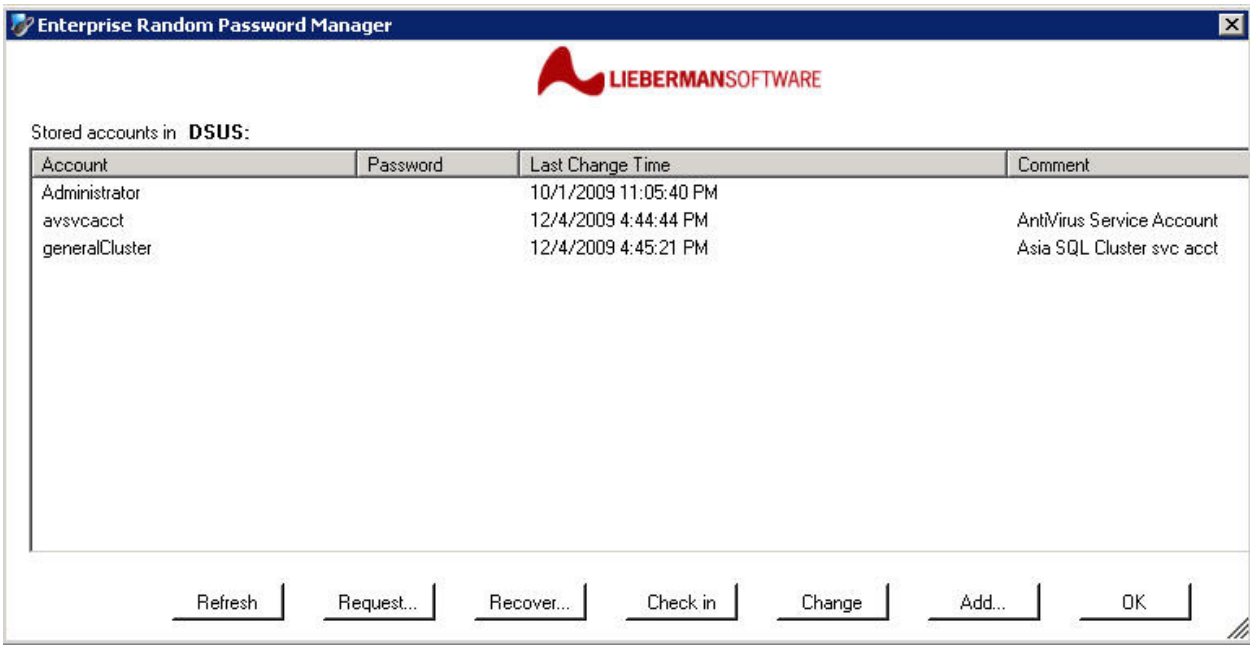
To recover a password expand the "Site Database\Computer Management\Collections\{NodeName}", right-click on the desired computer and from the 'Password Management' menu choose 'Recover Privileged Password'.



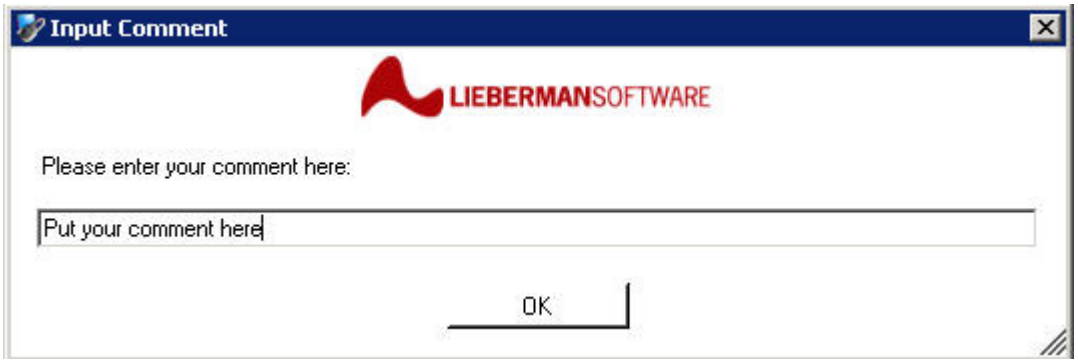
If integrated authentication is not configured, a prompt for a user name and password will appear. The account specified here must have been delegated rights to recover or request passwords in order to get past this point. If integrated authentication is enabled, this dialog will not be presented and the system will automatically authenticate using the currently logged on credentials.

Once logged in, a list of accounts available for the chosen system will be displayed. If there is a failure to login or there are no managed accounts for the specified system, a notification saying as much will be presented.

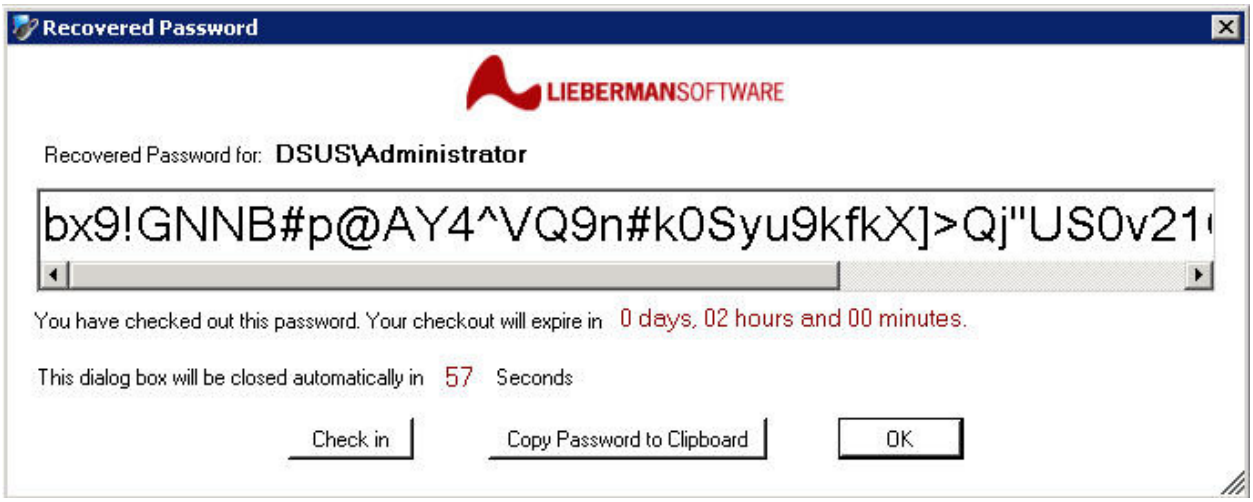
Select the account to be recovered and select the appropriate option to request the password for the account or simply recover the account.



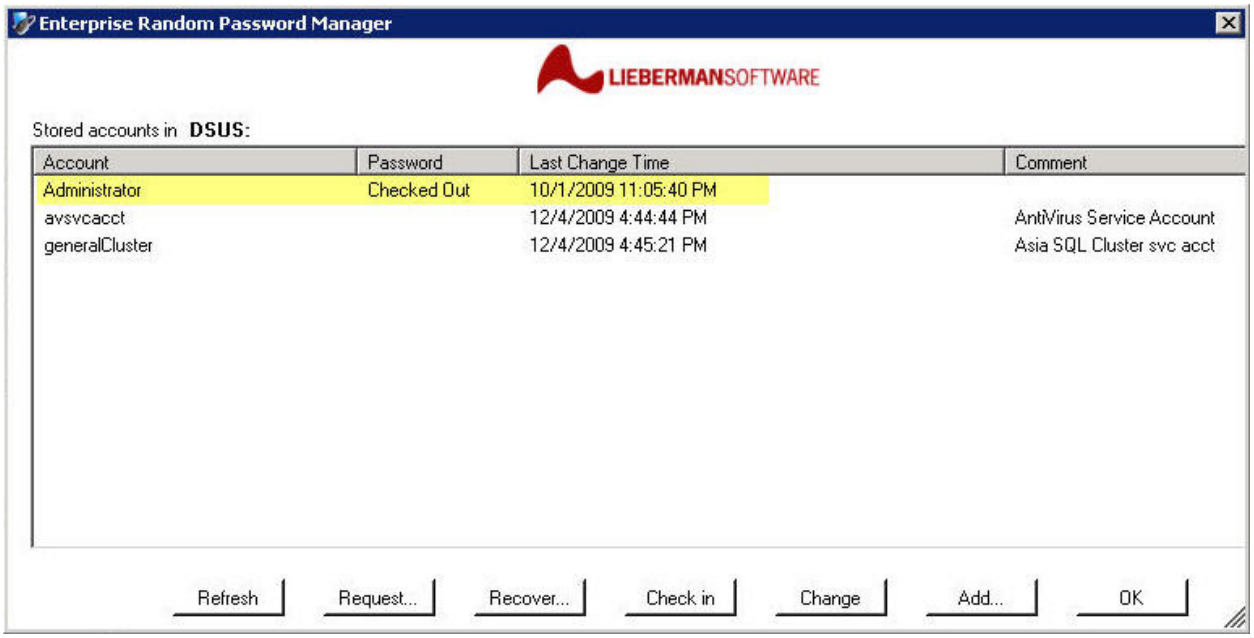
As is required by the password recovery website options, a prompt may appear asking for a check-out comment.



The password will then be displayed and checked out for the defined duration. Click OK to close the dialog or 'Check in' to check the password in and close the dialog. When checking in the password, per the account and website settings, the password may be triggered for immediate re-randomization.



Once the password is checked out, the status of the password will be set to 'Checked Out'.



To check a password back in from this dialog, highlight the account and select 'Check in'.

Additional accounts to be associated with the selected computer system may also be added from this dialog. Account entered here will be considered static accounts and will not be re-randomized following password recovery at a later time.

SCOM - Recovering Passwords

In order to be able to recover the password for an account being managed by ERPM/RPM, the system must also appear in the list of managed systems in the SCOM interface. If there are no stored accounts available when you attempt a recovery, you will be notified as such.

There are two possible reasons as to why a message indicating there are no stored accounts may appear:

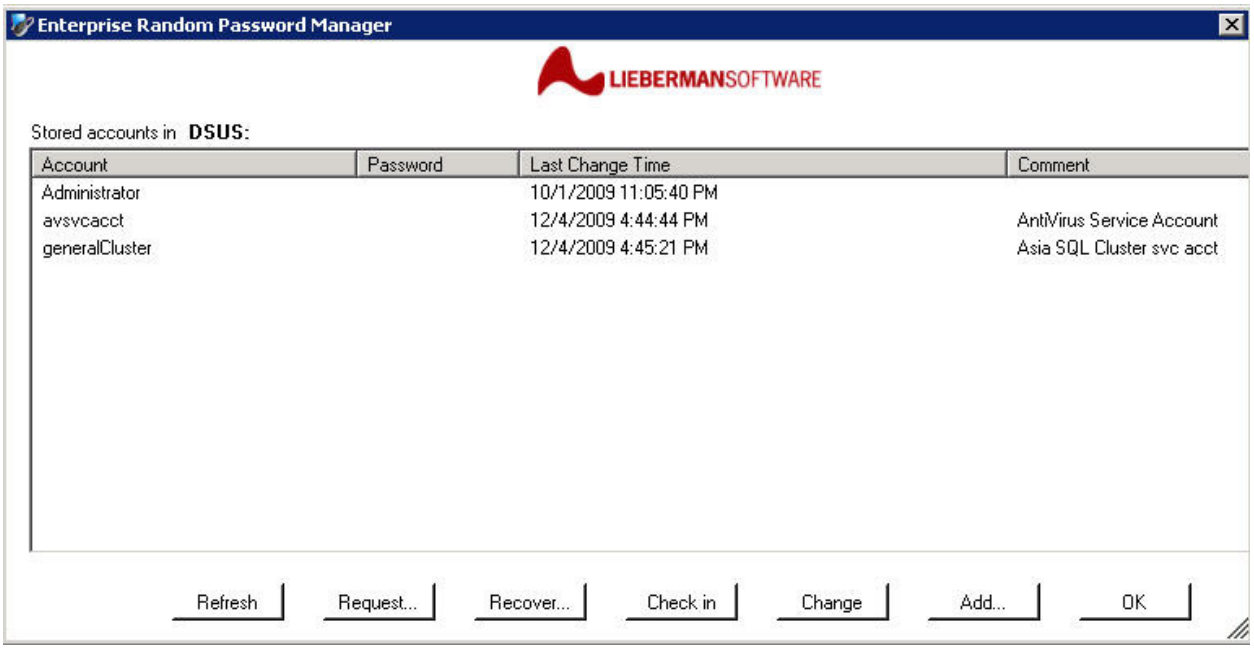
- There truly are no stored passwords
- The credentials used to login/recover the passwords does not have the ability to see any accounts on the selected system - see the ERPM/RPM web delegation rules.

To recover a password open the Monitoring section and select the 'Computers' node. Click on the desired computer and from the Actions pane choose '[Enterprise] Random Password Manager - Recover Privileged Password'.

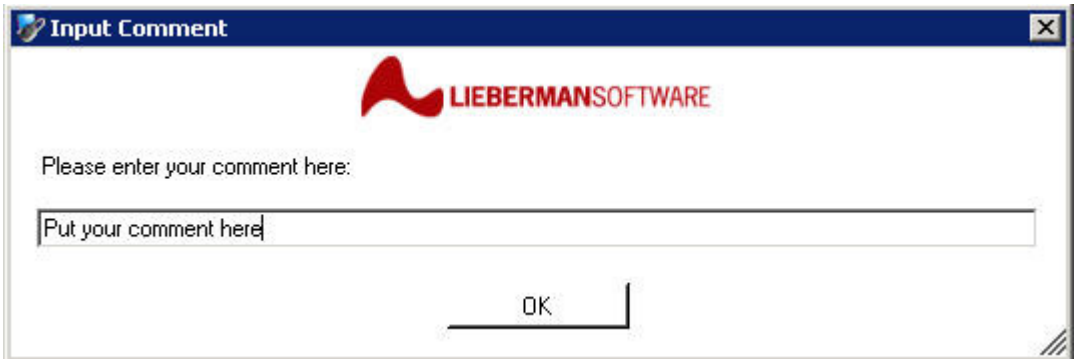
If integrated authentication is not configured, a prompt for a user name and password will appear. The account specified here must have been delegated rights to recover or request passwords in order to get past this point. If integrated authentication is enabled, this dialog will not be presented and the system will automatically authenticate using the currently logged on credentials.

Once logged in, a list of accounts available for the chosen system will be displayed. If there is a failure to login or there are no managed accounts for the specified system, a notification saying as much will be presented.

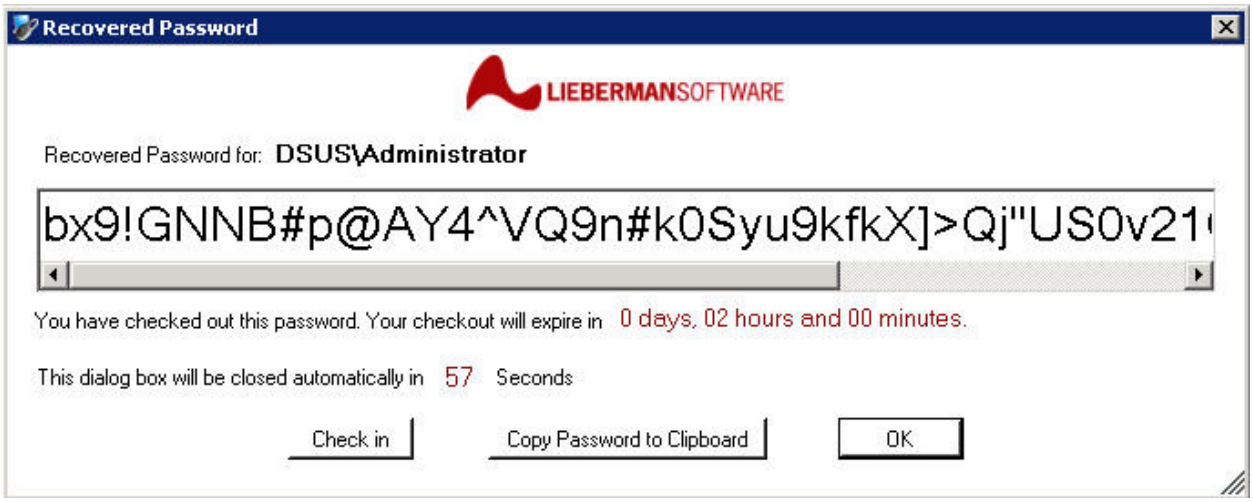
Select the account to be recovered and select the appropriate option to request the password for the account or simply recover the account.



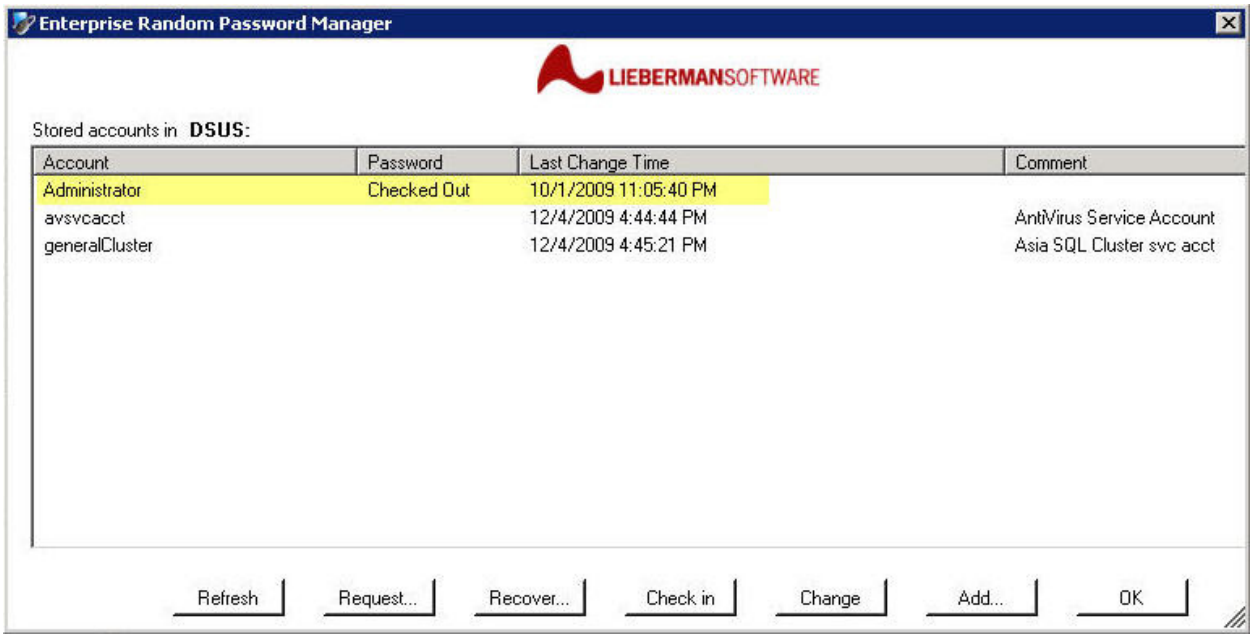
As is required by the password recovery website options, a prompt may appear asking for a check-out comment.



The password will then be displayed and checked out for the defined duration. Click OK to close the dialog or 'Check in' to check the password in and close the dialog. When checking in the password, per the account and website settings, the password may be triggered for immediate re-randomization.



Once the password is checked out, the status of the password will be set to 'Checked Out'.



To check a password back in from this dialog, highlight the account and select 'Check in'.

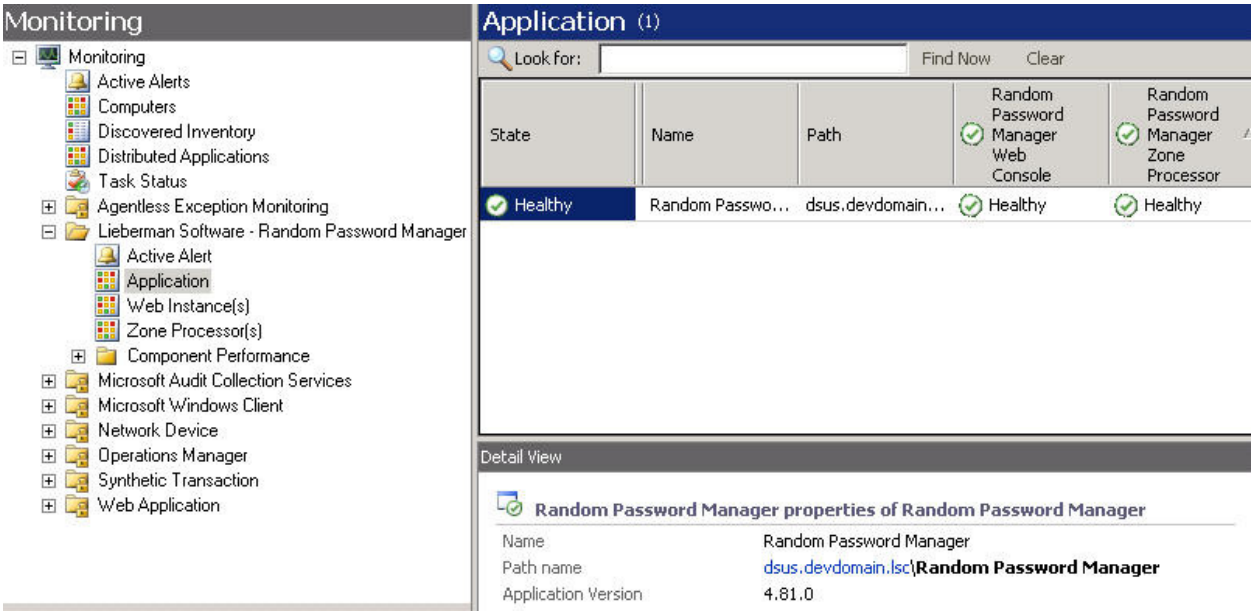
Additional accounts to be associated with the selected computer system may also be added from this dialog. Account entered here will be considered static accounts and will not be re-randomized following password recovery at a later time.

SCOM - Monitoring

SCOM can monitor the application components that comprise ERPM/RPM. When the management pack is installed a new node will appear in the monitoring pane called 'Lieberman Software - [Enterprise] Random Password Manager'. Under this node will be:

- Active Alerts - All alerts for all components of the solution
- Application - Information about the application including install path, registry location, database, etc
- Web Instance(s) - website pages and COM object
- Zone Processor(s) - default scheduling service and zone processors

In order for this monitoring to occur, the SCOM agent must be installed on each Windows system hosting an component, not just the main application server.



In the Application, Web Instances, and Zone Processors node, all components should come back healthy. If a component is not healthy, examine the active alerts and examine the links to see the state of the item exhibiting the error.

Index