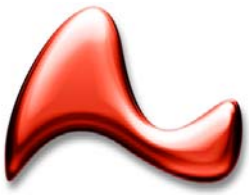
# Role-Based Access Controls in Lieberman Software's Privileged Identity Management Solutions

## Executive Summary

Lieberman Software's Privileged Identity Management Solutions: Enterprise Random Password Manager (ERPM) and Random Password Manager (RPM) received a major upgrade in version 4.81 (and later) that allows these two products to support Role Based Access Controls (RBAC) from virtually any LDAP directory on the market.

For organizations that use RBAC based management, this upgrade makes the implementation of a cross platform privileged identity management system radically simpler, and removes the previous product version's requirement to provide a Microsoft directory to support delegation of access.

This upgrade is also part of the most recent enhancements that provide authorization and authentication from all LDAP providers such as IBM, Sun, Oracle, Apache, Novell, OpenLDAP, HP and others.



LIEBERMANSOFTWARE™



© 2009 by Lieberman Software Corporation. All rights reserved. Rev. 20090901

## Contents




© 2009 by Lieberman Software Corporation. All rights reserved. Rev. 20090901

# Introduction

Lieberman Software provides **Role-Based Access Control** (RBAC) capabilities to version 4.81 and later of its privileged identity password management solution: **Enterprise Random Password Manager (ERPM) and Random Password Manager (RPM)**.

The previous versions of these products were tied exclusively to Microsoft Windows for authentication and authorization using Windows group memberships to derive rights. With the 4.81 release of our products, customers can also use role-based attributes (existing or new) from any LDAP directory of their choosing (including, but not limited to Microsoft Active Directory). Existing predefined roles in LDAP directories found in customer environments are immediately supported.

From a business perspective, many large organizations have adopted RBAC because of its simplification of access controls as well as its ability to support cross-platform system security management. RBAC also provides a consistent framework for IT auditors, regulators, and application developers.

## What is Role-Based Access Control?

"Security administration can be costly and prone to error because administrators usually specify access control lists for each user on the system individually. With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier." [1]

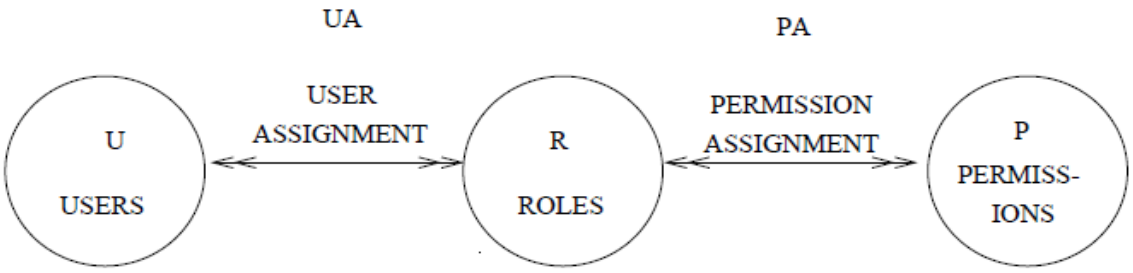



**Figure 1 - RBAC Associates Roles to Users and Roles to Permissions[1] – The ability to associate a role to multiple permissions independently of users simplifies administration. Picture from Sandu, Ferraiolo, Kuhn.**

[1] "The NIST Model for Role-Based Access Control: Towards A Unified Standard", Sandu, Ferraiolo, Kuhn. http://csrc.nist.gov/groups/SNS/rbac/documents/towards-std.pdf


© 2009 by Lieberman Software Corporation. All rights reserved. 

## When is RBAC Not Necessary?

Generally speaking, small organizations and some large organizations with simple business and access models, as well as simple/flat infrastructures do not require RBAC, or see significant advantages in its implementation. By assigning users to specific Windows groups (operating system groups) and associating specific permissions and rights to those same groups, most organizations can maintain reasonable security and audit ability (common case).

The important element that allows RBAC to be an optional component is the use of a common operating system such as Microsoft Windows and Microsoft applications being the core operating system and infrastructure for all business processes.

## Where is RBAC Required?

In heterogeneous IT organizations where a wide variety of operating systems, directories, authenticators, and applications are in use, only RBAC security can provide a common base of standards to control access in a standardized way.

From the point of view of a security auditor, such complex and non-standardized infrastructures are almost impossible to audit due to the vast amount of specialized knowledge needed and the sheer number of control points to monitor.

It is a foregone conclusion that mistakes will be made in such a complex environment that grants too much access to the wrong people for too long. Provisioning systems can automate group membership and per-user permission grant/revoke operations, but in reality, most of the provisioning systems end up being incomplete in their coverage or fail to cover 100% of the changes in an organization (i.e. employee transfers, promotions, leaves of absences, retirement, temporary projects) properly.

Add to this scenario the lack of formal tools to see the entire enterprise security as a whole, RBAC systems and applications that support RBAC control becomes a necessity to not solve the problems, but at least improve the situation. In the case of heterogeneous environment, they are required as the only security glue to tie vendor solutions together.

The NIST web site has an excellent page filled with links pointing to different RBAC implementation white papers and standards references:

http://csrc.nist.gov/groups/SNS/rbac/standards.html

## How is Role-Based Authentication Implemented in ERPM?

Role based access controls are implemented for both console and web based access of ERPM. The RBAC facility is used to perform role to permission mapping. The pre-existing system performs Windows groups to permission mapping. The following screen shot shows both Windows groups and roles mapped to specific rights.


© 2009 by Lieberman Software Corporation. All rights reserved.

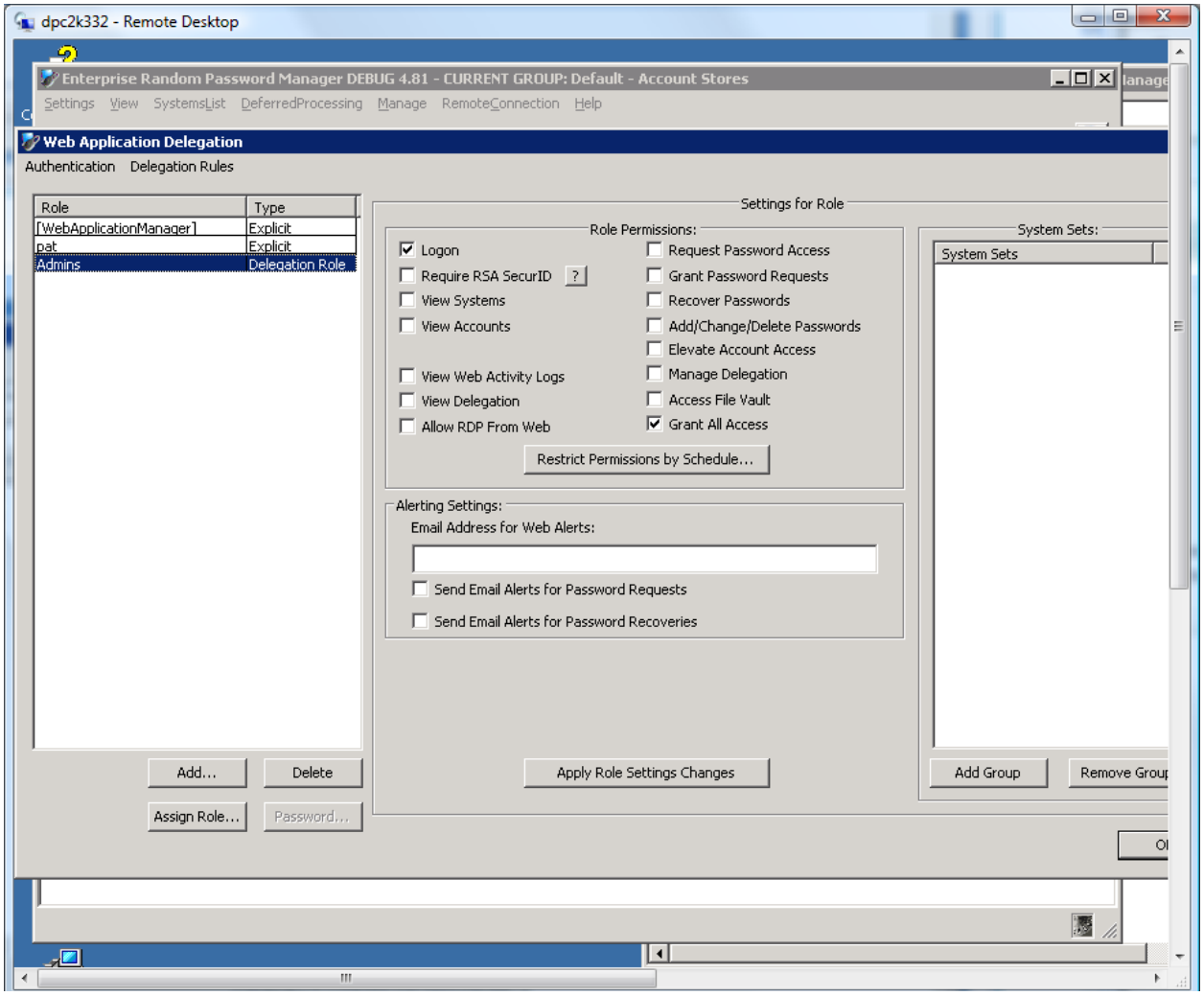



**Figure 2 - Mapping "Admins" Role to Logon Right**

Note that the role for a specific user is derived from the directory used to authenticate that user. Multiple roles may be picked up for a user and roles may be accumulated. Roles are typically inserted into existing user account definitions by existing provisioning systems. ERPM has the ability to retrieve the existing roles and allows an organization to map them to rights and permissions within ERPM via a graphical user interface.

The method of role pickups is controlled on a per-directory basis. The LDAP objectClass may be mapped uniquely for each directory used in a customer environment. This allows the peaceful coexistence between multiple directories.


© 2009 by Lieberman Software Corporation. All rights reserved.

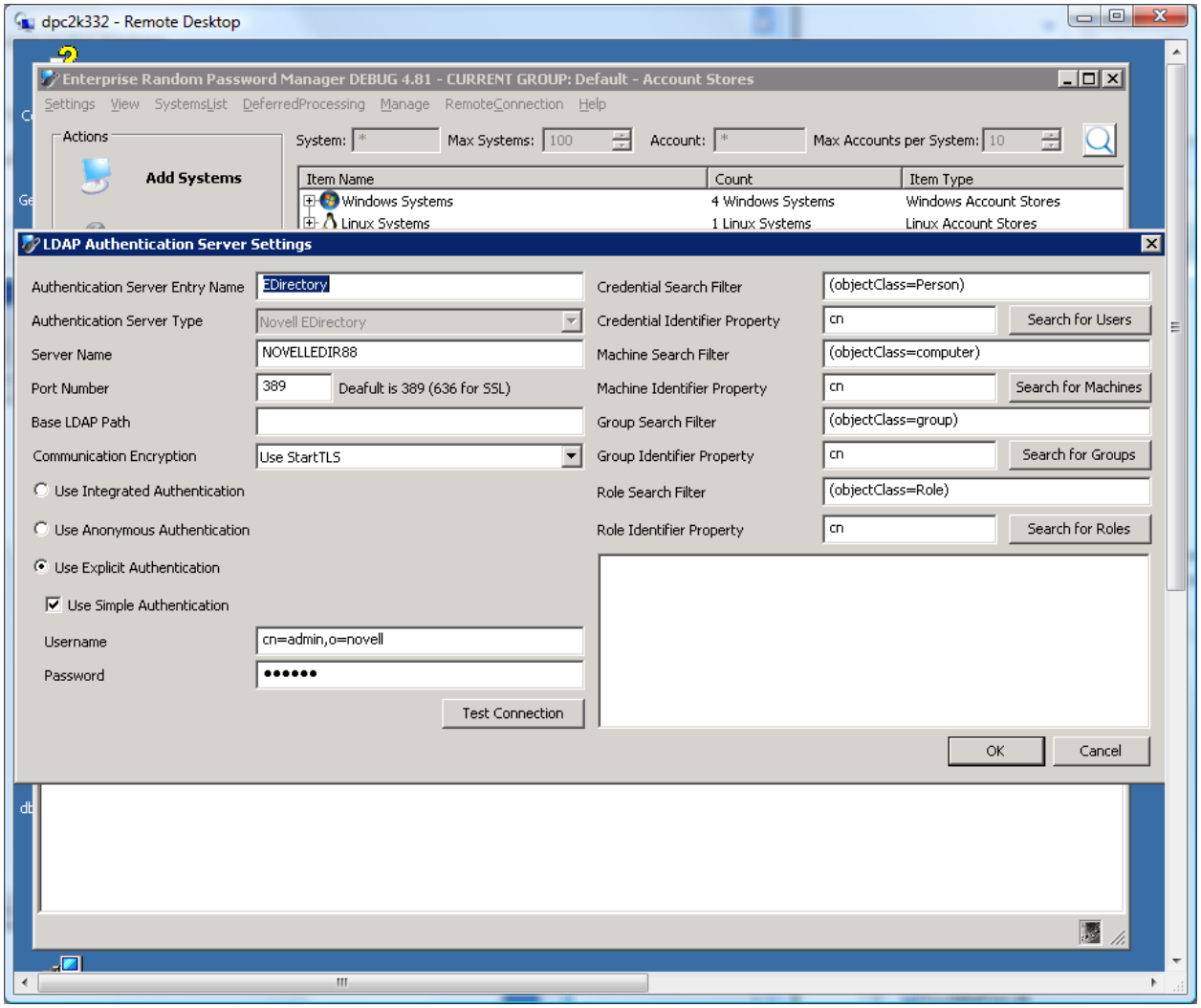



**Figure 3 - The "Role Search Filter" controls the pickup name used to determine the roles for each user.**

## Summary

Role based access controls represent an emerging standard for large enterprises that seek to simplify security and access control management. The current version of ERPM supports RBAC on an unlimited number of concurrent directories with complete flexibility as to the number of roles as well as allowing any number of ERPM permissions to be mapped to any role.

Note that based on the search criteria provided for roles, both flat and hierarchical role accumulation is possible.


© 2009 by Lieberman Software Corporation. All rights reserved.

## Next Steps

If you would like to see how ERPM or RPM can use role-based attributes to help you manage privileged access in your enterprise, please contact Lieberman Software for a fully functional product evaluation. Trial software is available at no cost to qualified organizations. For more information, email **info@Liebsoft.com**.

# About Lieberman Software

Lieberman Software Corporation, established in 1978 as a software consultancy, has been a profitable, management-owned organization since its inception. The company provides privileged identity management and security management solutions that secure the multi-platform enterprise. By automating time-intensive IT administration tasks, Lieberman Software increases control over the computing infrastructure, reduces security vulnerabilities, improves productivity, and helps ensure regulatory compliance.

Lieberman Software is a Microsoft Gold Certified Partner and has technical partnerships with other industry leaders such as Cisco, Novell, Red Hat, Hewlett-Packard, IBM, RSA, Oracle and Intel. The company is headquartered in Los Angeles, CA, and maintains a regional office in Austin, TX. All product development, testing, and support operations are based in the United States.

For more information, visit **www.liebsoft.com**
or call 800-829-6263 (USA and Canada) or 01-310-550-8575 (International).


© 2009 by Lieberman Software Corporation. All rights reserved. 