



## Securing Application-to-Application Passwords with Enterprise Random Password Manager™

**Privileged identities** are the so-called “keys to the kingdom” of IT, granting elevated permission to access sensitive data and change configuration settings of virtually every hardware and software component on your network.

**Enterprise Random Password Manager (ERPM)**, the privileged identity management solution from Lieberman Software, safeguards and manages the privileged identities found throughout your infrastructure, including:

- ▶ **Super-user login accounts** used by individuals to change configuration settings, run programs, and perform other administrative duties.
- ▶ **Service accounts** that require privileged login IDs and passwords to run.
- ▶ **Application-to-application passwords**, the credentials used by web services, line-of-business applications, custom software, and virtually every other type of application to connect to **databases**, **middleware**, and **other application tiers**.

### Risks of Unmanaged Application Passwords

Absent proactive security controls, hard-coded application credentials present an elevated security risk. That’s because these passwords may seldom change and can become known to more and more individuals over time – making them an easy target for abuse. And, reused or cryptographically weak, hard-coded application passwords can provide an easy launch point for hackers and malicious programs to gain access to your network.

Fortunately ERPM manages application passwords across your cross-platform enterprise. Unique for its ability to manage embedded privileged account credentials throughout your application tiers, ERPM helps you replace hard-coded privileged account passwords found in the widest range of applications

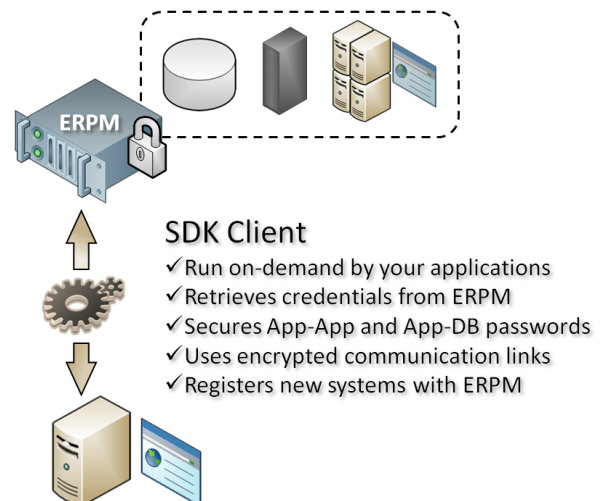
with cryptographically secure, frequently changed password credentials.

### Securing Application Credentials

ERPM continuously secures embedded passwords in web application tiers, packaged software programs, line-of-business applications, custom programs and more – automatically changing embedded passwords according to rules that you define for complexity and change frequency, and synchronizing all changes across interdependent tiers to prevent lockouts and service disruptions.

ERPM synchronizes changes across your application tiers in these ways.

- ▶ **An SDK**, included at no additional cost, for securing passwords embedded in Windows, Linux, and UNIX applications. Applications run the SDK client code when needed to retrieve current credential information programmatically, over an encrypted connection, from ERPM’s secure data store. The SDK also enables newly-deployed systems running your applications to register programmatically with ERPM. This enables you to enforce password security policies immediately upon first deployment of your new systems.





The SDK is provided in multiple formats including a Java applet, executable (CLI), COM object, and direct URL reference and runs only when needed to enable client access. It supports PKI, integrated authentication, and other methods to operate with virtually any authentication environment.

- ▶ **Automatic string replacement** with custom propagation to secure passwords according to your policies for complexity, uniqueness and change frequency in application files including database configuration files, *web.config*, compiled binary files and others.
- ▶ **Launching arbitrary processes** to find and update credentials – executing both your custom processes and scripts supplied by third-party software vendors to update credentials according to your security policies.

Because ERPM issues application credentials programmatically and enrolls new assets immediately, you'll avoid service lockouts while closing a significant security hole on your network.

### Part of a Comprehensive Solution

In addition to securing the privileged credentials in use by your application tiers, ERPM safeguards super-user login accounts, privileged service accounts, and more. ERPM provides the industry's only Iron-to-Application<sup>SM</sup> management of privileged accounts on physical and virtual operating systems, clustered computers, network appliances, out-of-band management devices, hypervisors, middleware, and line-of-business applications. Comprehensive multi-platform support includes Windows, Linux, UNIX, OS/390, AS/400, IOS appliances and many others.

ERPM offers these key benefits:

- ▶ **Improved security** by mitigating the threat of common and weak account passwords leading to peer-level network access, unauthorized users and malware attacks.

- ▶ **Increased productivity** through fast setup and low management overhead, made possible by automated account discovery and authentication directly with every major directory service – ERPM eliminates account lockouts and cascading systems failures following credentials changes by auto discovering every place a password is used.
- ▶ **Reduced costs and uncertainty of regulatory compliance audits** achieved by continuous updating all privileged account passwords, logging of each password change and account access, comprehensive, customizable Auditing and Compliance reports.
- ▶ **Proven scalability** through use of the customer's choice of industry-standard MS SQL Server or Oracle Databases and an extensible Zone Processing architecture that enables reliable policy enforcement and password propagation over slow and unreliable WAN links and across DMZs and multiple network domains.
- ▶ **Time-saving automation** using multi-threaded processes that discover and secure privileged accounts everywhere on the network.

### To Learn More

Contact Lieberman Software at **(800) 829-6263** or **sales@liebsoft.com** for more information or to request a no-obligation software trial.

Or visit us online at **www.liebsoft.com**.