



Privileged Identity Management via the ArcSight® Interface

Organizations fail security audits and suffer costly data breaches because their privileged identity passwords go unmanaged. Your organization's privileged credentials grant access to sensitive data and allow users to change the configuration of virtually every server, database, web server, application and network appliance.

Conventional identity access management software can't detect or control privileged identities. That's why you need **Enterprise Random Password Manager™** (ERPM) to continuously discover, update, store, and enable secure recovery of every local, domain, and process account password in the enterprise. ERPM detects each location that privileged account credentials are used in services, tasks, applications and more. It then secures these credentials and propagates the changes everywhere they're needed.

ERPM is **Common Event Format (CEF) certified** for the **ArcSight® Security Information and Event Management (SIEM)** platform to give you enhanced application layer monitoring, visibility and management of privileged accounts right from the familiar ArcSight interface.

How Can ERPM Help You?

Stay Secure As Your Environment Changes

- ▶ **Continuous Discovery.** As your organization deploys new hardware and software applications, ERPM continuously discovers and secures new privileged identities to eliminate security risks.
- ▶ **Stronger Password Security.** When malicious programs and unauthorized users attempt to gain access to your computers and applications, they encounter the robust, unique, frequently changing credentials propagated by ERPM.
- ▶ **Immediate User Recognition.** Whenever the role of any staff member changes, ERPM instantly allows or denies privileged access based on up-to-the-minute data it takes from your Role-Based Access Control system.

Eliminate Tedious, Error-Prone Tasks

- ▶ **Improved Staff Efficiency.** When your security policies require frequent changes to privileged passwords, ERPM discovers and changes these credentials immediately, eliminating hours of tedious, error-prone work.
- ▶ **Fewer Service Disruptions.** As your integrated IT services expand, ERPM detects new application interdependencies and simultaneously deploys all changed credentials to avoid service disruptions and lockouts.



(5 OUT OF 5 STARS)

"ENTERPRISE RANDOM PASSWORD MANAGER FROM LIEBERMAN SOFTWARE IS AN EXTREMELY POWERFUL TOOL WHICH AUTOMATICALLY DISCOVERS, UPDATES, STORES, AND ALLOWS SECURE RECOVERY OF EVERY PRIVILEGED ACCOUNT PASSWORD THROUGHOUT THE ENTERPRISE."

— SC MAGAZINE



- ▶ **Faster Emergency Access.** No matter when authorized IT personnel need privileged access to perform routine tasks or emergency fire call repairs, ERPM grants the credentials securely and without delay, according to roles that you predefine, through a console that's accessible from any web-enabled device.

Reduce IT Audit Cost and Uncertainty

- ▶ **Easier Compliance.** When standards such as PCI DSS, SOX and HIPAA require you to enforce privileged password security, ERPM continuously discovers and strengthens the privileged accounts on all hardware in your enterprise.
- ▶ **Comprehensive Audit Trails.** Each time authorized IT staff request privileged access for routine maintenance or emergency fire-call repairs, ERPM creates an authoritative audit trail showing the requestor, target system and account, date and time, location, and purpose of the request.
- ▶ **Efficient Compliance Reporting.** Whenever you are required to prove compliance, ERPM gives you detailed reports that eliminate the manual effort it otherwise takes to document that all of your privileged accounts are secure.

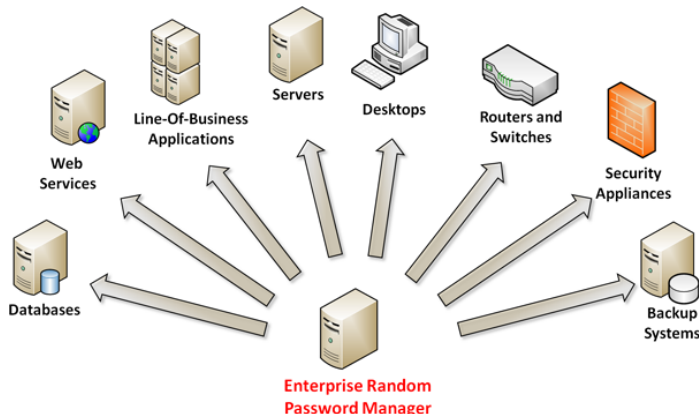


Account Name	System	Account	Usage
ADMINISTRATOR	SERVER	ADMINISTRATOR	Administrative tasks
SYSTEM	SERVER	SYSTEM	System maintenance
...

Customizable Audit Reports Eliminate Compliance Uncertainty

Secure and Scalable

ERPM creates unique, cryptographically complex passwords for each privileged account and changes them as often as your policies require. These unique credentials mitigate the threat of unauthorized peer-to-peer access and ensure the confidentiality of each privileged account password until an authorized user checks it out. Credentials are secured in an AES-256 bit encrypted database with an option for PKCS #11 hardware encryption.



ERPM Continuously Discovers and Strengthens Privileged Account Passwords on All Platforms

ERPM continuously discovers, strengthens and controls the privileged credentials on every server and workstation platform; on datacenter hardware such as routers, switches, application accelerators and security appliances; and on line-of-business applications, Web services, databases and middleware, backup services, identity access management and systems management applications. It integrates with leading helpdesk and business applications through a provided SDK, and its configurable Event Sink feature can alert and report user and administrator actions through third-party Security Information and Event Management (SIEM) frameworks.

Authorized personnel can recover passwords from any web-enabled device allowing fast, fully-audited retrieval of privileged credentials and automated approvals of each request. Credentials are re-randomized immediately after use, and administrators maintain delegated control over the accounts and systems that each user can access.

Comprehensive Platform Support

ERPM continuously discovers, strengthens and controls the privileged credentials on every server and workstation platform; on datacenter hardware