

## Secure the Administrator Account Passwords in Your Enterprise

### *Audit and Control Access to Your Powerful Administrator and Root Accounts*

#### KEY FEATURES

##### Randomized Passwords

Automate the frequent creation of unique, cryptographically-complex passwords for each account, including firecall accounts.

##### Password Retrieval

Retrieve current passwords on demand through a secure, delegated and audited web interface.

##### Password Auto-Roll

Re-randomize passwords after their temporary usage periods expire.

##### Temporary Credentials

Issue temporary privileges to users needing to install applications and perform systems administration.

##### Cross-Platform Support

Supports Windows, Linux and UNIX systems; mainframe servers; SQL Server, MySQL and Oracle databases; Juniper and Cisco devices; Dell DRAC cards, and more.

##### Hardware Encryption

Offers hardware-based encryption with any PKCS#11 hardware device.

##### Zero-Touch Install

Deploys without installing agents or scripts on client systems.

##### Password Workflow

Utilizes request/approval workflow process to ensure that only authorized users can access sensitive passwords.

To simplify the task of systems administration, most IT groups deploy servers, workstations and devices with identical local account names and passwords. While convenient for the IT department, this tactic unfortunately results in a fundamentally insecure organization. A malicious user with access to any machine on the network can easily obtain the local credentials from one system, decrypt them, and gain peer-level access to every other system in the enterprise.

### Random Password Manager

The solution to this common credentials dilemma is to use unique, cryptographically complex passwords for each privileged account in the network. With **Random Password Manager (RPM)**, a systems administrator can automate frequent randomization of all administrator and root account passwords, assuring that no two machines have identical credentials. And with security best practices and government regulations requiring that administrator and root account passwords be updated at regular intervals, Random Password Manager helps organizations maintain compliance with **HIPAA, Sarbanes-Oxley, PCI DSS** and other regulatory standards.

### Password Retrieval

But frequently updating privileged account passwords is only part of the task. Because these passwords are needed for critical systems administration operations, Random Password Manager provides a **secure and delegated web interface for retrieving current passwords**. It can be used to delegate **who can access passwords** and for what length of time.

Random Password Manager can also automatically **re-randomize the passwords after the temporary access period expires**, so there is no risk of a password being available long-term. Delegation to retrieve passwords can be designated per machine or for a group of machines.





## Trouble Ticket Lifecycle

Random Password Manager integrates with leading **trouble ticketing systems** to control access to privileged credentials, ensuring that only authorized staff can access sensitive systems, with an approved purpose, for a limited time. All administrator password checkout/check-in transactions become **part of the trouble ticket record, are audited and are available for review** by IT management and auditors.

Random Password Manager does so by verifying that the ticket exists, confirming that the ticket number is for the requested system, validating that the ticket is open, and authenticating that the user who opened the ticket has permission to log into the console. When these criteria are established, the trouble ticket is logged into Random Password Manager. Only then is the privileged account password released to the requestor.

## Enterprise Deployment

Random Password Manager is a multi-threaded product that **does not require agents or scripts** to be deployed on client systems. It's **certified for Microsoft** Windows 7, Hyper-V, Server 2008, and Vista and is **RSA SecurID** certified. The product supports every version of Windows dating back to NT, as well as Linux, UNIX, OSX, OS/390, and AS400 systems; Juniper and Cisco network devices; and Dell DRAC cards. Customers can choose to utilize either Microsoft SQL Server or Oracle Database 11g as the backend data store. The web interface **supports all standard web browsers** on all platforms, and web-enabled Windows mobile devices.

## Random Password Manager Can Help You:

- ▶ **Mitigate Risks** – Protect against unauthorized personnel attempting to access your sensitive data.
- ▶ **Secure Datacenter Changes** - Quickly change common default passwords on new hardware devices and software introduced into your IT environment.
- ▶ **Protect Against Personnel Changes** - Update and audit access to administrator account passwords, securing these credentials against former employees and contractors.
- ▶ **Reduce Audit Costs** – Verify the security of privileged account passwords to regulatory compliance auditors.

## Try It Free

Qualified organizations can receive a fully functional trial version of Random Password Manager at [www.liebsoft.com/rpmdemo](http://www.liebsoft.com/rpmdemo)

## Comprehensive Privileged Identity Management

RPM is just one solution in our line of privileged identity management products. For even more functionality, including auto discovery and categorization of all privileged accounts, see **Enterprise Random Password Manager™**.

*"RANDOM PASSWORD MANAGER AUTOMATICALLY GENERATES UNIQUE, COMPLEX ADMINISTRATOR PASSWORDS FOR EACH SYSTEM IN THE ENTERPRISE. THE RANDOMIZATION IS AUTOMATED FROM A SINGLE CONSOLE FOR ALL MANAGED SYSTEMS ACCORDING TO SCHEDULES ESTABLISHED BY THE SYSTEM MANAGER."*

— DAVE KEARNS  
CONTRIBUTING EDITOR  
NETWORK WORLD