



Secure Local Account Management for the Cross-Platform Enterprise

Randomize and Recover Local Account Passwords Stored on Servers, Workstations, Routers, Firewalls, and Databases

KEY FEATURES

RANDOMIZED PASSWORDS

Automate the creation of unique, complex passwords for each privileged account, including firecall accounts.

PASSWORD RECOVERY

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

PASSWORD AUTO-ROLL

Randomize retrieved passwords to a different value after their temporary usage periods expire.

TEMPORARY CREDENTIALS

Issue temporary privileges to users needing to install applications and manage their systems.

ENCRYPTED DATA

Employs AES-256-bit data encryption, with optional hardware-based encryption at FIPS 140-2 levels 2 and 3.

CROSS-PLATFORM SUPPORT

Supports Windows, Linux, UNIX, OSX, OS/390 and AS/400 systems; SQL Server, MySQL, Sybase and Oracle accounts; and Juniper and Cisco IOS devices.

DELEGATED USERS

IT staff controls user access to local account passwords.

PASSWORD WORKFLOW

Requires a request/approval workflow password checkout process.

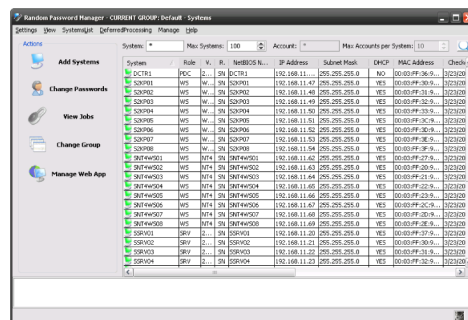
PASSWORD STORE

Store user and administrator passwords, and important documents and files, in encrypted data stores.

To simplify the task of systems management, most organizations deploy servers and workstations with a common local account name and password. While this is a convenience for the IT department, it unfortunately results in a fundamentally insecure organization. A user with physical access to any machine on the network can easily extract the local credentials from one system, decrypt them, and gain peer-level access to the enterprise.

RANDOMIZED PASSWORDS

The solution is to use unique and cryptographically complex passwords for each account in the network. With Random Password Manager™, an administrator can schedule periodic randomization of all administrator and root account passwords, assuring that no two systems have identical credentials. And with security best practices and government regulations requiring that local passwords be updated at regular intervals, Random Password Manager helps organizations maintain compliance with HIPAA, Sarbanes-Oxley, PCI, and other regulatory standards.



Randomize and recover local account passwords across all systems in the enterprise.

PASSWORD RECOVERY

But updating passwords is only part of the solution. Because local passwords must be available for critical systems administration operations, Random Password Manager provides a secure and delegated web interface to recover current passwords. The product controls who can retrieve passwords and for what length of time. Passwords are automatically re-randomized after the temporary period expires, so there is no risk of a password being available for long term use. Random Password Manager can also force immediate password check-in, show the history of all passwords, verify that the passwords it created are still valid, and provide phonetic spelling of passwords.

TEMPORARY ADMINISTRATOR CREDENTIALS

Users are granted only the appropriate level of temporary privileges needed to safely accomplish routine systems administration tasks, such as installing applications or device drivers. Providing temporary administrator credentials for limited users reduces the risk of end-users with administrative rights harming their systems, either through malicious or accidental acts.



KEY BENEFITS

ENTERPRISE SECURITY

Prevents one compromised local password from threatening the security of the entire network.

REDUCE THREATS

Provides temporary administrator credentials for limited users, minimizing the risks of users running with administrative privileges.

REGULATORY COMPLIANCE

Helps organizations meet and maintain regulatory compliance standards by auditing the effectiveness of password management controls.

INCREASE PRODUCTIVITY

Eases 24/7 Help Desk burden of issuing and expiring administrator credentials and installing applications for users.

PASSWORD STORE

Delegated users can store all of their passwords in an encrypted database and recover them when necessary without involving the IT staff or Help Desk. Administrators can archive passwords for all IT components in the enterprise, such as hardware firewalls or network devices. The encrypted stores can also be utilized for delegated storage of important documents and files.

LOGGING

All password changes, verifications, and recoveries — as well as program logons — are logged into a relational database. Information can be sorted and extracted to CSV files and provided to security compliance auditors.

SECURITY

Credentials that are stored or transmitted with Random Password Manager are secured through SSL data encryption to the browser, storage in a SQL relational database, and military-level AES-256-bit data encryption in the database. The product also enables hardware-level encryption when used with any PKCS #11 hardware provider.

ENTERPRISE SUPPORT

Random Password Manager is Certified for Microsoft Windows Hyper-V, Server 2008, and Vista. It supports every version of Windows dating back to NT 4.0. The product can also handle all versions and distributions of Linux, UNIX, and OSX. Randomization of Microsoft SQL Server, MySQL, and Oracle database accounts and Juniper and Cisco IOS devices is also supported.

Random Password Manager utilizes a SQL Server-based architecture, allowing it to scale to the largest enterprise environments. It does not require any scripts or agents to be deployed on client systems, and it does not require any additional hardware to be added to the IT infrastructure. An optional zone processing feature improves performance in geographically dispersed environments, or in environments with security-restricted DMZ systems where standard communications are not allowed.

“ [Random Password Manager]... creates unique passwords for all systems that a user must access, thereby preventing a single password vulnerability from daisy chaining across systems. ”

ALEX WOODIE
IT Jungle
Senior Editor

